
# EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR

TESIS DOCTORAL PRESENTADA POR
LUIS OSWALDO ORDÓÑEZ PINEDA

Programa de doctorado en Ciencias Sociales y Jurídicas

DIRECTOR:

Dr. ANTONIO TRONCOSO REIGADA

Catedrático de Derecho Constitucional de la Universidad de Cádiz

**2021**

**ÍNDICE**

**CAPÍTULO I: REFERENTES TEÓRICOS PARA EL ESTUDIO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES** ----------7

**1.** Introducción ----------7
**2.** Planteamiento del problema ----------14
**3.** Antecedentes del derecho a la protección de datos personales en el contexto latinoamericano ----------17
**4.** El derecho fundamental a la protección de datos personales como hecho, valor y norma ----------22
**5.** Reflexiones desde la teoría del Derecho Constitucional ----------28
**5.1** Aproximación al concepto neoconstitucional ----------30
**5.2** Derivación del derecho a la protección de datos personales según la teoría de los derechos humanos ----------34
**6.** Conceptualización de la protección de datos personales como un derecho fundamental ----------37
**6.1** Definición del contenido del derecho fundamental a la protección de datos personales ----------43
**6.2** Los datos sensibles o especialmente protegidos ----------49
**6.3** El control de la información personal y ejercicio de los derechos ----------52
**6.4** *El habeas data* como garantía para la protección de datos personales ----55
**7.** El derecho fundamental a la protección de datos personales en la Constitución ecuatoriana ----------60
**7.1** Referencia al pensamiento bolivariano en el proceso constitucional de Latinoamérica ----------60
**7.2** Del *habeas* data al derecho fundamental a la protección de datos personales en la Constitución de Ecuador ----------63
**7.3** La Reforma Constitucional de 2008 en Ecuador ----------70
**7.4** La Corte Constitucional en la definición del derecho fundamental a la protección de datos: precisiones sobre los derechos de acceso, rectificación, cancelación y oposición ----------81
**7.5** Algunas precisiones finales sobre el derecho fundamental a la protección de datos personales. Referencia a los artículos 66.19 y 92 de la Constitución ecuatoriana ----------87

**CAPÍTULO II: ESTUDIO COMPARADO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES** ----------96

**1.** Introducción ----------96
**2.** Reconocimiento del derecho fundamental a la protección de datos personales en Latinoamérica. Hacia un modelo de integración regional según la Guía Legislativa para los estados miembros de la OEA ----------102
**2.1** El derecho fundamental a la protección de datos personales en Latinoamérica ----------108

**2.1.1** Guatemala ----------109
**2.1.2** Nicaragua ----------113
**2.1.3** Brasil ----------116
**2.1.4** Colombia ----------121
**2.1.5** Paraguay ----------125
**2.1.6** Perú ----------128
**2.1.7** Venezuela ----------134
**2.1.8** Bolivia ----------139
**2.1.9** Chile ----------142

**2.2** Especial referencia a la situación de Argentina, Uruguay y México ------146

**2.2.1** Argentina ----------151
**2.2.2** Uruguay ----------157
**2.2.3** México ----------160

**3.** Enmarque del derecho fundamental a la protección de los datos personales en la Unión Europea. Referencia a su regulación en España ----------164

**3.1** La Carta de Derechos de la Unión Europea y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE ----------169
**3.2** El caso de España ----------174

**CAPÍTULO III: ESTUDIO DE LA NORMATIVA QUE DESARROLLA EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR, DESDE UNA PERSPECTIVA SECTORIAL** ----------180

**1.** Introducción ----------180
**2.** Régimen sectorial que desarrolla el derecho fundamental de protección de datos personales en Ecuador ----------187
**2.1** La protección de datos personales en el Sector de la Salud ----------187
**A.** Código de Ética Médica ----------187
**B.** Ley Orgánica de la Salud ----------190
**2.2** La protección de datos personales en el Sector Social ----------197
**A.** Ley de Seguridad Social ----------197
**B.** Código de la Niñez y la Adolescencia ----------204
**2.3** La protección de datos personales en el Comercio Electrónico ---------209
**A.** Ley de Comercio Electrónico, Firmas y Mensajes de Datos ------209
**2.4** La protección de datos personales en la Administración de Justicia ---215
**A.** Código de la Niñez y la Adolescencia ----------215
**B.** Código Orgánico Integral Penal ----------220
**C.** Código Orgánico General de Procesos ----------223
**2.5** La protección de datos personales en el Régimen Tributario ----------226
**A.** Ley Orgánica de Régimen Tributario ----------226

**B.** Código Tributario ----------230
**2.6** La protección de datos personales en el Régimen Electoral ----------232
**A.** Código de la Democracia ----------232
**2.7** Regulación de la información sobre solvencia patrimonial y de crédito 236
**2.8** Especial referencia a la protección de datos personales en la Administración pública: Ley del Sistema Nacional de Registros Públicos, Ley Orgánica de Comunicación y Ley Orgánica de Telecomunicaciones ----------240
**A.** Ley del Sistema Nacional de Registros Públicos ----------241
**B.** Ley Orgánica de Comunicación ----------245
**C.** Ley Orgánica de Telecomunicaciones ----------248

**CAPÍTULO IV: ANÁLISIS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN ECUADOR. REFERENCIAS A LOS PROYECTOS DE LEY DE 2016 Y 2019** ----------255

**1.** Introducción ----------255
**2.** Estudio del objeto, ámbito de aplicación y definiciones contenidas en la Ley general en Ecuador ----------261

**2.1** Objeto del marco general de protección de datos personales ----------261
**2.2** Ámbito de aplicación ----------267
**2.3** Principales definiciones ----------277

**2.3.1** Base o bancos de datos (ficheros) ----------278
**2.3.2** Consentimiento del titular (consentimiento del interesado) ----------280
**2.3.3** Datos de carácter personal ----------285
**2.3.4** Datos sensibles (especialmente protegidos) ----------289
**2.3.5** Disociación de datos (procedimiento de disociación y/o seudonimización) ----------294
**2.3.6** *Habeas data* (ejercicio de los derechos de acceso, rectificación, cancelación y oposición) ----------297
**2.3.6.1** Limitación al tratamiento, portabilidad y decisiones individuales automatizadas ----------306
**2.3.7** Responsable del tratamiento de la información ----------314
**2.3.8** Encargado del tratamiento ----------316
**2.3.9** Titular de los datos ----------317
**2.3.10** Tratamiento de datos ----------321
**2.3.11** Usuario de datos ----------324

**CAPÍTULO V: LOS PRINCIPIOS Y DERECHOS DE LA PROTECCIÓN DE DATOS, COMO GARANTÍAS DEL TRATAMIENTO DE LA INFORMACIÓN PERSONAL** ----326

**1.** Introducción ----------326
**1.1** El principio de licitud ----------328
**1.1.1** Condiciones para el consentimiento ----------337

**1.2** El principio de pertinencia ----------344
**1.3** El principio de veracidad ----------347
**1.4** El principio de confidencialidad e integridad: El deber de secreto y la seguridad de los datos ----------350
**1.5** El principio de transparencia e información al interesado ----------357
**1.6** El principio de responsabilidad proactiva ----------360
**1.7** Tratamiento de categorías especiales de datos personales ----------362

**2.** Derechos de los Titulares ----------367

**CAPÍTULO VI: OBLIGACIONES DEL RESPONSABLE Y DEL ENCARGADO DEL TRATAMIENTO** ----------383

**1.** Introducción ----------383

**2.** Obligaciones del responsable ----------386

**2.1** Obligaciones generales ----------387
**2.2** Protección de datos, desde el diseño y por defecto ----------395
**2.3** Seguridad de los datos personales ----------400
**2.4** Evaluación de impacto en el tratamiento de datos y consulta previa -404
**2.5** El delegado de protección de datos ----------408
**2.6** Crítica a otras obligaciones enmarcadas en el proyecto de ley de 2016 - ----------413

**3.** Obligaciones del encargado ----------417

**CAPÍTULO VII: LA PROTECCIÓN DE DATOS PERSONALES DE LOS MENORES Y NUEVOS DERECHOS DIGITALES** ----------428

**1.** Introducción ----------428
**2.** Los entornos digitales y el cambio de paradigma en la protección de datos personales ----------431
**3.** La corresponsabilidad: El papel de la familia ----------439
**4.** Derechos de los menores en la Ley Orgánica de Protección de Datos Personales en Ecuador ----------448
**5.** La necesidad de políticas públicas y programas para la promoción de los derechos y obligaciones relativas al derecho fundamental a la protección de datos personales, en especial de los niños, niñas y adolescentes ----------455

**CAPÍTULO VIII: LAS AUTORIDADES DE CONTROL Y SUPERVISIÓN, FRENTE A LA TUTELA DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES** ----------465

**1.** Introducción ----------465
**2.** Naturaleza de las autoridades de control y supervisión ----------469

**3.** Las garantías formales de independencia ----------478
3.1 Referencia especial a la autonomía financiera ----------488
**4.** Funciones de la autoridad de control ----------492
**A.** Función normativa o reguladora ----------493
**B.** Función de control de ficheros, de tutela de derechos y de ejercicio de la potestad sancionadora ----------496
**C.** Función de publicidad y registro de ficheros ----------502
**D.** Función de promoción del derecho a la protección de datos ----------504

**CONCLUSIONES** ----------509

**BIBLIOGRAFÍA** ----------522

**ANEXOS**

# CAPÍTULO I: REFERENTES TEÓRICOS PARA EL ESTUDIO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

## 1. Introducción

En las últimas décadas del siglo XX, el derecho fundamental a la protección de datos personales ha tenido un reconocimiento, tanto en los Tratados y Acuerdos Internacionales, como en las Constituciones de los distintos países[1]. Así, por ejemplo, en el ámbito internacional, se destaca el Protocolo de 2018 que actualiza el Convenio 108 del Consejo de Europa y lo adapta al Reglamento General de Protección de Datos[2]. Esto se ha traducido en un desarrollo legislativo de este derecho fundamental tendente a regular el tratamiento de la información personal,

[1] En el marco internacional, el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal –y su Protocolo Adicional relativo a autoridades de supervisión y transferencias internacionales–; y la Directiva 95/46/CE –del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos– representan instrumentos que reconocen principios y derechos sobre el tratamiento de datos de datos personales. El Convenio 108 es una norma internacional que garantiza el derecho fundamental a la protección de datos de carácter personal, mientras que la Directiva 95/46 –actualmente derogada por el Reglamento (UE) 2016/679– tuvo como principal objetivo que los Estados miembros de la Unión Europea, garanticen la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. Sobre la importancia de estos instrumentos internacionales, Cfr. Pérez Tremps, P., La jurisdicción constitucional y la integración europea, *REDE*, núm. 29, 2009, pp. 19-48; Mangas Martín, A., *El Derecho de la Unión y el Derecho español*, en Mangas Martín, A., y Liñán Nogueras, D. J., Instituciones y Derecho de la Unión Europea, 6a ed. Tecnos, Madrid, 2010, pp. 467-486; Pérez Tremps, P., *Las fuentes internacionales y supranacionales*, en Derecho Constitucional, I. 8a ed., Tirant lo Blanch, Valencia, 2010, pp. 95-115. Cfr. también Heredero Higueras, M., *La Directiva Comunitaria de protección de los datos de carácter personal*. Tecnos, Madrid, 1998; Arenas Ramiro, M., *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2006, pp. 191-376; y Téllez Aguilera, A., *La protección de datos en la Unión Europea*. *Divergencias normativas y anhelos unificadores*, Edisofer, Madrid, 2002, pp. 329-349. Por otra parte, se destacan, –aunque con menor desarrollo en los ordenamientos jurídicos latinoamericanos–, el Memorándum de Montevideo (2009), sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes; los Principios de privacidad y protección de datos personales (2015) de la OEA; y los Estándares de protección de datos personales (2017) para los Estados Iberoamericanos.

[2] Como se expuso en la Propuesta de Decisión del Consejo, el Protocolo modificativo "tiene por objeto ampliar el ámbito y aumentar el nivel y la eficacia de la protección de datos garantizada en virtud del Convenio 108". Cfr. Propuesta de DECISIÓN DEL CONSEJO que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Disponible en: https://tinyurl.com/y6rv45fw.

por parte de las Administraciones Públicas, como por parte de las entidades privadas.

Por un lado, se afirma que el reconocimiento de la protección de datos de carácter personal, como un derecho fundamental, nace de los problemas que plantea el tratamiento automatizado de la información personal, a través, de las TICs. Así, "el elemento determinante de la necesidad o interés esencial sobre el que se construye es el proceso tecnológico, principalmente, el derivado de los avances que resultan de la combinación de las virtualidades de la informática y de las telecomunicaciones"[3]. Por tanto, este nuevo derecho –de tercera generación– surge de la ampliación del marco de protección de la persona, frente al tratamiento de sus datos personales en una sociedad informatizada.

Como señala la doctrina y jurisprudencia internacional, este derecho se materializa como un instituto de garantía de otros derechos fundamentales. Si bien, su tutela se conecta con el respeto del derecho a la intimidad, tanto personal como familiar; el derecho fundamental a la protección de datos personales, al atribuir a la persona el control de su información de carácter personal; se considera como un instituto de garantía de otros derechos. Por ejemplo, a la luz de la Carta de Derechos Fundamentales de la Unión Europea y de la Constitución Europea, se reconoce este derecho "en preceptos distintos al derecho a la protección de la vida privada. Este carácter autónomo frente al derecho a la intimidad (…) es también consecuencia de su carácter instrumental en relación con otros derechos fundamentales"[4].

La realidad es que las Administraciones Públicas y la sociedad, en general, se enfrentan al manejo de grandes cantidades de información de carácter personal, por lo que su tratamiento obliga al Estado a aprobar un marco de regulación y garantía de los derechos fundamentales, que se pueden ver afectados por el tratamiento de la información personal.

---

[3] Pablo Lucas Murillo de la Cueva y José Luis Piñar Mañas, El *derecho a la autodeterminación informativa* (Madrid-México: Fontamara S.A, 2011), 15.

[4] Antonio Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, (Valencia: Tirant lo Blanch, 2010), 73.

En el ámbito de la Unión Europea, el Convenio 108 del Consejo de Europa se instituyó como "el primer instrumento internacional vinculante en materia de protección de datos personales en los sectores público y privado, que no sólo ha reconocido sino que ha fijado los elementos principales del contenido del derecho fundamental a la protección de datos personales"[5]. Por ello, la normativa del Consejo de Europa significa el punto de referencia para articular en los Estados un marco de regulación, que recoja principios y salvaguardias para la protección del derecho a la autodeterminación informativa[6].

A esto, se suma la importancia de la Directiva 95/46/CE, relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que intentó "armonizar el respeto y la tutela de los derechos de las personas con el necesario tratamiento de los datos personales como elemento que impulsa el progreso de la economía y del mercado"[7]. Así también la Carta de Derechos Fundamentales de la Unión Europea (2000/C 364/01) reconoce a este derecho fundamental de manera autónoma y "ha servido para que el TJCE se pronuncie expresamente sobre el derecho fundamental a la protección de datos en la labor de interpretación de la Directiva 95/46/CE sobre Protección de Datos Personales"[8].

Finalmente, el Tratado de Lisboa (2007/C 306/01) que "suprime la distinción entre pilares –pasando el ámbito policial y judicial de la cooperación a la integración– y

[5] Antonio Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, Nro. 43 (2012): 25-184.

[6] En todo caso, la Propuesta de Decisión del Consejo para el Protocolo modificativo del Convenio 108 destacó que "el Convenio modernizado garantizará un alto grado de protección, al tiempo que deja un margen de flexibilidad a las Partes por lo que se refiere a la incorporación de sus disposiciones al ordenamiento jurídico interno. De esta manera, se hará atractiva la adhesión al Convenio 108 modernizado para aquellos países, también fuera de Europa, que están pensando en crear o reforzar sus sistemas de protección de datos. Su incidencia en la práctica será previsiblemente mucho mayor que la del Convenio 108 vigente, tanto desde el punto de vista de su ámbito de aplicación como de las obligaciones dispuestas en él". Cfr. Propuesta de DECISIÓN DEL CONSEJO que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Disponible en: http://data.consilium.europa.eu/doc/document/ST-9766-2018-INIT/ES/pdf.

[7] Ana Isabel Herrán, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, (Madrid: Dykinson, 2002), 123.

[8] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 175.

que ha dado un valor vinculante a la Carta de Derechos Fundamentales de la Unión Europea"[9]; y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos –en adelante RGPD–, que ha derogado la Directiva 95/46/CE[10], suponen un nuevo esquema de la regulación, dentro de la Unión Europa que "podemos decir que pasa de la gestión de los datos al uso responsable de la información"[11].

Por otra parte, salvo casos excepcionales, la situación en la que se encuentra Latinoamérica, respecto al desarrollo normativo-regional, se presenta deficiente a diferencia de la Unión Europea. Como ha señalado el Comité Jurídico Interamericano de la Organización de Estados Americanos en 2015; el enfoque normativo en la región se ha caracterizado por ser heterogéneo e incompatible, con las exigencias que plantea este derecho fundamental en el ámbito internacional[12].

Considerando el marco de regulación europeo, en materia de protección de datos personales, es imprescindible que "la normativa internacional de protección de datos incorpore una visión más amplia que acoja el ámbito geográfico americano y de Asia-Pacífico"[13]. Bajo este paradigma, el derecho a la protección de datos

[9] Ibíd., 176.

[10] La aprobación del Reglamento (UE) 2016/679 "evidencia la irreversible *europeización* de la estrategia pública de protección de los derechos fundamentales frente a la tecnología que ya fue iniciada por la Directiva 95/46, que el artículo 8 CDFUE ya consagró al elevar a rango constitucional europeo un derecho fundamental autónomo a la protección de datos y que la jurisprudencia europea (singularmente, del TJUE) ha contribuido a consolidar inequívocamente en sucesivos pronunciamientos que han configurado una jurisdicción garante de los derechos fundamentales frente a los avances tecnológicos en la era digital". Cfr. Artemi Rallo Lombarte, "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)", *UNED: Revista de Derecho Político*, Nro. 100 (2017), 639-669.

[11] José Luis Piñar Mañas, "Introducción. Hacia un nuevo modelo europeo de protección de datos", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 14.

[12] El Informe del Comité Jurídico Interamericano, relativo a los "Principios de privacidad y protección de datos personales" destaca que "en las Américas no parece haber surgido un enfoque "regional" uniforme y coherente. La contribución más significativa que puede hacer el Comité es aprovechar las experiencias y los logros de otras regiones, teniendo en cuenta, al mismo tiempo, la situación de nuestro propio continente, a fin de formular una propuesta de marco legal que los Estados de las Américas puedan usar para abordar este campo crucial".

[13] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 48.

personales tiende a caracterizarse como un derecho global, que exige de la comunidad internacional una respuesta equilibrada, en el objetivo de salvaguardar el poder de disposición y control de la información personal, atendiendo, fundamentalmente, los riesgos que plantea la sociedad de la información y del conocimiento[14].

Teniendo en cuenta la normativa europea, en los últimos años, el marco latinoamericano ha decido, progresivamente, incorporar una visión más global, compatibilizando su normativa a estándares internacionales, a partir de las necesidades de integración comercial y transferencias internacionales de datos personales[15]. Lógicamente, estos procesos de integración exigen de los Estados adoptar medidas de seguridad y garantías suficientes en el tratamiento de la información personal, que aseguren su reconocimiento como países con un nivel adecuado[16].

---

[14] Nos parece importante señalar que, el RGPD destaca que "el tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad" –considerando 4–.

[15] Precisamente, el marco de regulación latinoamericano se está asemejando en gran medida al modelo europeo. Como precisa la OEA, "la guía se basaría en los 12 principios adoptados anteriormente por el Comité, con algunas modificaciones menores, teniendo en cuenta los diversos conjuntos de directrices preparados en la Unión Europea, la OCDE, APEC, etc. El objetivo es explayarse en los principios, proporcionando un contexto más amplio y orientación a los Estados Miembros a fin de facilitar la elaboración de Leyes nacionales". Cfr. Organización de Estados Americanos (OEA). Disponible en: https://tinyurl.com/y3ajwhqd. Así también en los Estándares de protección de datos personales (2017) para los Estados Iberoamericanos, que corresponden a la actividad que viene desarrollando la Red Iberoamericana de Protección de Datos (RIPD); se desprende que la elaboración y aprobación de dichos Estándares contó "con el apoyo de la propia Comisión Europea y han supuesto un verdadero revulsivo para la regulación de la protección de los datos personales en la región (…) En la elaboración de los Estándares Iberoamericanos también se han tomado como referencia otros instrumentos internacionales y emblemáticos en materia de protección de datos personales como son las Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos; el Convenio número 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo; el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico, y el Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, entre otros". Cfr. Red Iberoamericana de Protección de Datos (RIPD). Disponible en: https://tinyurl.com/yy7df8jp.

[16] Es preciso anotar que, en el siguiente capítulo se abordarán los avances que, en el contexto latinoamericano, han desarrollado varios países de la Comunidad Andina en materia de protección

Asumiendo que el derecho a la protección de datos personales es una libertad que tiene una significativa trascendencia en las relaciones globales entre países; en nuestra región, debe destacarse la importancia que tienen la "Guía legislativa" de 2015 de la OEA, plasmada en los "Principios de privacidad y protección de datos personales"[17]; y los "Estándares de protección de datos personales" de 2017 para los Estados Iberoamericanos[18]. A pesar de no existir una exigencia taxativa para la aplicación de estos instrumentos, un ejemplo del nivel adecuado de protección regional, conforme a estándares internacionales y siguiendo el modelo europeo, significa el marco jurídico adoptado por Argentina y Uruguay, por el que han recibido reconocimiento internacional, tomando en consideración que "su legislación reconoce principios y derechos de protección de datos, establece autoridades de control independientes y prevé los necesarios recursos administrativos y jurisdiccionales"[19].

Esta realidad plantea en los Estados establecer regímenes jurídicos de garantía, que cumplan con los requerimientos que la sociedad demanda hoy en día; y que,

---

de datos personales. Hasta ahora, la principal novedad es que –siguiendo la experiencia europea–, las sesiones del Comité Jurídico Interamericano y propuesta del Departamento de Derecho Internacional han desarrollado un modelo de "Guía legislativa", a partir de principios estandarizados a nivel internacional para la protección de la información de carácter personal. Así, se considerará la necesidad de generar una integración regional homogénea para la protección de datos personales.

[17] Mediante el 86 período ordinario de sesiones del Comité Jurídico Interamericano de la OEA, en sesiones celebradas en marzo del 2015, se adopta por consenso la denominada "Guía legislativa" para los Estados Miembros fundamentada en los doce principios aprobados en 2012. La finalidad de estos principios, plasmados en la Guía legislativa de la OEA, es "establecer un marco para salvaguardar los derechos de la persona a la protección de los datos personales y a la autodeterminación en lo que respecta a la información". Cfr. Guía legislativa de la OEA. Disponible en: https://tinyurl.com/y358v8zv.

[18] Los "Estándares de protección de datos personales para los Estados Iberoamericanos" fueron aprobados por unanimidad el 20 de junio de 2017, en el marco del XV Encuentro Iberoamericano de Protección de Datos de la Red Iberoamericana de Protección de Datos (RIPD). Ecuador forma parte de la RIPD, en calidad de país observador. A partir del concepto global que el derecho fundamental a la protección de datos personales tiene en el contexto europeo, debe resaltarse que dichos Estándares, como se expone en el considerando 10, se promueven a partir de "la adopción de instrumentos regulatorios que garanticen, por una parte, la protección de las personas físicas con relación al tratamiento de sus datos personales; y por otra, el libre flujo de los datos personales que actualmente constituyen la base para el desarrollo, fortalecimiento e intercambio de bienes y servicios en una economía global y digital, sobre los cuales se erigen las economías de los Estados Iberoamericanos". Cfr. Estándares de protección de datos personales para los Estados Iberoamericanos. Disponible en: https://tinyurl.com/y8wvqzb2.

[19] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 182.

por consiguiente, prescriban que la Administración Pública y entidades privadas, en general, sometan sus sistemas de tratamiento de datos personales a las exigencias derivadas del respeto al derecho fundamental a la protección de datos personales[20].

En este contexto, teniendo como eje central el derecho a la protección de los datos de carácter personal, este capítulo, en su primera parte, se dedica a conceptualizar las bases que promueven su desarrollo, desde las exigencias que plantea el avance de las tecnologías de la información y comunicación. Para este fin, un aporte interesante se desprende del estudio de la teoría tridimensional del derecho, la cual aborda el derecho a la protección de datos como hecho, valor y norma.

En una segunda parte, precisamos algunas reflexiones, desde la teoría del Derecho Constitucional. Apreciaremos la derivación del derecho a la protección de datos, desde la teoría de los derechos humanos y el neoconstitucionalismo andino. Por tanto, desarrollaremos conceptos y definiciones que se atribuyen a la protección de datos y al *habeas data,* como una garantía jurisdiccional para la tutela de la información de carácter personal.

Finalmente, nos dedicaremos al estudio e identificación de las bases que promovieron, en Ecuador, el reconocimiento constitucional de la protección de datos personales, como un derecho fundamental, a partir de la Reforma de 2008.

En suma, este capítulo contribuye a generar una aproximación sobre la naturaleza de este derecho fundamental que, como una institución jurídica de reciente aparición en el contexto latinoamericano, exige del Derecho una respuesta integral acorde a las necesidades globales que la sociedad plantea. En estos términos, proponemos estudiar el derecho a la autodeterminación informativa, atendiendo los

[20] Como señala Antonio Troncoso, el reconocimiento internacional sobre niveles adecuados de protección, exige que los ordenamientos jurídicos regulen transferencias internacionales de datos, lo cual "abre la posibilidad de que los países iberoamericanos se conviertan en un espacio donde sean posibles inversiones y actividades empresariales que impliquen transferencias de datos personales, convirtiendo esa región en un espacio más competitivo para el ámbito de las TIC". Cfr. Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 182.

avances teóricos y enfoques constitucionales que, en la actualidad, requiere el derecho a la protección de datos personales.

## 2. Planteamiento del problema

Al configurarse como un derecho fundamental –a lo que no cabe discusión, desde el punto de vista constitucional, jurisprudencial y doctrinario–; y tomando en consideración los distintos avances tecnológicos y comerciales, es necesario determinar los elementos esenciales que componen el concepto “derecho a la protección de datos personales”.

Los conflictos en los que se ven envueltos los juristas en el discernimiento y la construcción de verdades jurídicas comprenden una labor que requiere una debida fundamentación, apoyada en la reconstrucción de los modelos e instituciones jurídicas, que permiten obtener conciencia plena sobre su naturaleza. El saber jurídico se encuentra caracterizado por desarrollar instituciones jurídicas nuevas, que contienen definiciones ambiguas. Por ello, es ineludible profundizar y cambiar nuestras percepciones del derecho y de la sociedad. Basándonos en la teoría tridimensional del derecho –hecho, valor y norma–, evidenciaremos las principales características y elementos esenciales que se desprenden del derecho a la protección de datos personales.

La sociedad ha experimentado diversos avances sociales, políticos, económicos y tecnológicos, a partir de los cuales, el Derecho, “como ciencia social llamada a regular y ordenar los comportamientos humanos, no ha resultado inmune a las transformaciones sociales causadas por la revolución tecnológica y ha sufrido las modificaciones inevitables y necesarias para someter las nuevas conductas vinculadas al cambio tecnológico”[21]. Así, frente a estos cambios, el Derecho no puede desentenderse. Su funcionalidad está encaminada a proteger los derechos individuales y colectivos, tanto para el hombre, como para la comunidad en general. Es evidente que el derecho a la protección de datos emerge de la necesidad de

[21] Rallo Lombarte, “De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)”, 642.

salvaguardar el derecho de las personas, respecto al tratamiento de su información de carácter personal. En una sociedad, en la que predomina el desarrollo tecnológico, el tratamiento de datos personales presenta nuevos riesgos, los cuales afectan a la dignidad de las personas; "es por ello que se plantea la necesidad de que desde el ordenamiento jurídico se otorgue al ciudadano el amparo debido, frente a la potencial agresividad de la informática"[22].

La doctrina ha identificado principios generales, mecanismos de control y supervisión –en suma, modelos de regulación–, para la protección de los datos personales, contenidos en instrumentos internacionales y en los ordenamientos jurídicos de los Estados, que han recibido reconocimiento internacional. Desde luego, estos presupuestos tienen como principal objetivo articular un marco jurídico que, de manera integral, respondan a los nuevos planteamientos sociales y tecnológicos.

Conforme a las disposiciones del RGPD, destacamos la importancia de:

> Los principios de privacidad desde el diseño y por defecto, la aproximación a la protección de datos basada en el análisis de riesgos, la figura del Delegado de protección de datos, el fortalecimiento de los códigos de conducta, la exigencia de llevar un registro de las actividades del tratamiento, la regulación de las medidas de seguridad, y un largo etcétera (...) Pero junto a estos elementos, que sin duda acercan el modelo del Reglamento al estadounidense, el legislador europeo ha reivindicado con fuerza el papel protagonista de las autoridades de control independientes, como pieza clave e imprescindible del contenido mismo del derecho fundamental a la protección de datos[23].

La evolución que ha experimentado en las últimas décadas el derecho a la protección de datos personales es diversa y se caracteriza, principalmente, por el desconocimiento que existe en la sociedad sobre su contenido, a consecuencia de las dificultades que podría comprender su alcance. Sobre este aspecto, apuntamos que:

> La relativa complejidad del lenguaje utilizado por el legislador, tributario en buena parte de terminologías y expresiones procedentes de directivas europeas, no es una ayuda para superar esta dificultad. Como tampoco lo es la tendencia de parte de los especialistas y de

[22] María Rodríguez Pérez, "Tridimensionalismo jurídico y protección de datos personales frente a su tratamiento automatizado", *Saberes: Revista de estudios jurídicos, económicos y sociales*, Vol. 1 (2003): 1-14.
[23] Piñar Mañas, "Introducción. Hacia un nuevo modelo europeo de protección de datos", 14.

> las instituciones de garantía a servirse de conceptos difíciles de comprender para la mayor parte de las personas[24].

En este orden, parece conveniente reconstruir las bases y fundamentos que han llevado a considerar el reconocimiento de la protección de datos personales como un derecho fundamental. Por ello, es indispensable "volver sobre los aspectos esenciales de este derecho y, en particular, sobre las fuentes que legitiman los tratamientos y los principios que le inspiran. Es decir, sobre los elementos que son más genuinamente característicos de este derecho fundamental"[25].

En el desarrollo y cambios de paradigma de los derechos fundamentales, sus esquemas de tutela, garantía, promoción y difusión no pueden encaminarse por sí solos. Precisan que, a consecuencia de los avances tecnológicos y necesidades globales, sus fundamentos aseguren confianza en la ciudadanía y seguridad jurídica, a través, de la aplicación de normas legales claras. Por tanto, destacamos la necesidad de un estudio detallado sobre los fines mismos del derecho, particularmente, del derecho a la protección de datos personales. En todo caso, estimando que, "técnicamente, es posible confeccionar una información que proporcione conclusiones sobre el comportamiento, ideología, aficiones, enfermedades, etcétera de la persona y que, identificándola con ella afecte a su entorno personal, social o profesional en los límites de su intimidad"[26]; sobre la base del constitucionalismo contemporáneo, es fundamental que los sistemas jurídicos garanticen la tutela efectiva y la vigencia de los derechos, por medio de un orden de justicia, equidad y pleno respeto de la dignidad de las personas.

Estas exigencias, "imponen a la teoría jurídico-política una reflexión sobre las libertades que ya no puede transitar por los cómodos carriles prestablecidos por una larga historia doctrinal e institucional"[27]. Por consiguiente, es necesario cuestionar, exponer y argumentar las nuevas perspectivas que proyecta, en la actualidad, el

[24] Pablo Lucas Murillo de la Cueva, "La protección de los datos de carácter personal en el horizonte de 2010", *Anuario Facultad de Derecho – Universidad de Alcalá*, Nro. 2 (2009):131-142.
[25] Ibíd., 140.
[26] Rodríguez Pérez, "Tridimensionalismo jurídico y protección de datos personales frente a su tratamiento automatizado", 4.
[27] Antonio Pérez Luño, *La tercera generación de derechos humanos*, (Navarra: Aranzadi, 2006), 89.

derecho fundamental a la protección de datos. Para este fin, precisamos realizar un análisis del paradigma que supone su protección, frente al desarrollo de las nuevas tecnologías, en relación a los procesos globalizadores en el mundo moderno.

Evidentemente, planteamos que los presupuestos jurídicos, que componen este instituto de garantía, tienen que ser consecuentes con el respeto de la dignidad de las personas. Así, "el momento es, pues, particularmente importante y requiere, junto a la realización del balance de lo conseguido, el diseño de un planteamiento de futuro comprometido con la más plena realización del derecho"[28]. A continuación, se expone el contexto que representa el derecho a la protección de los datos, desde la teoría tridimensional y constitucional del derecho, a fin de precisar su naturaleza, objeto y garantía como un derecho fundamental.

## 3. Antecedentes del derecho a la protección de datos personales en el contexto latinoamericano

No solo para quienes tienen la tarea de administrar justicia, sino para todas las personas, un problema de gran relevancia es la interpretación de las normas, los principios, e instrumentos jurídicos que han sido adoptados de otros contextos. En materia de protección de datos, "puede agregarse que las previsiones constitucionales son muy generales, dejando así mucho margen para la interpretación judicial, por lo que al ser aplicados a casos concretos pueden generarse decisiones ambiguas o equivocadas, generando así falta de certeza legal"[29]. Esta realidad puede ser consecuencia de la falta de criterios del legislador para crear normas apegadas en técnicas de argumentación jurídica y sustentadas, sobre todo, en una realidad social cierta.

Gran parte del ordenamiento jurídico latinoamericano –diríamos que mucho más en Ecuador–, forma parte de una tradición jurídica sustentada en la integración

[28] Lucas Murillo de la Cueva, "La protección de los datos de carácter personal en el horizonte de 2010", 142.
[29] Valeria Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", *Revista Transparencia y Sociedad – Consejo para la Transparencia de Chile*, Nro. 5 (2017):13-31.

normativa de Leyes de otros contextos o realidades. Así, se origina una suerte de dispersión normativa que, carente de un modelo jurídico específico, conlleva, evidentemente, a errores de interpretación normativa. A esta perspectiva, se suma "el desconocimiento que la mayor parte de las personas tienen sobre los peligros derivados del acceso por terceros a los datos que les identifican o permiten identificarlos cuando no afectan directamente a su vida íntima"[30]. Lógicamente, la falta de reconocimiento constitucional y desarrollo de una legislación, que regule el derecho a la protección de datos personales, afecta también a ese desconocimiento por parte del legislador. En este aspecto, "esa circunstancia, sin duda preocupante, es más llamativa cuando de los poderes públicos se trata, por su vinculación positiva a la Ley y al Derecho"[31].

Ahora bien, en el caso de Estados que cuentan con una normativa vinculada a la protección de la información de carácter personal, el problema radica en la ausencia de mecanismos de prevención y concienciación ciudadana, sobre la importancia de mantener un control adecuado de los datos personales en la era digital.

> En este contexto, la conclusión a la que se debe llegar, una vez que se ha reconocido el derecho fundamental a la protección de datos, no puede ser otra que la del fortalecimiento de la tutela que aporta a los individuos y la insistencia en su contenido sustantivo. Para ello, son, sin duda, muy importantes cuantos esfuerzos se hagan desde las instituciones llamadas directamente a preservarlo para imponer su respeto, bien por las vías del fomento y el acuerdo, bien por las de la coacción[32].

Bajo estas consideraciones, estimamos la necesidad de crear espacios que faciliten el desarrollo de una cultura de responsabilidad digital en entornos tecnológicos que, integrando la intervención del Estado y la sociedad, procure el respeto de las libertades que se desprenden del tratamiento de la información personal. A esto, le llamaríamos un modelo de protección integral, basado en la corresponsabilidad.

Nos parece que son dos causas las que en las últimas décadas han originado preocupación y debate sobre el derecho fundamental a la protección de datos personales. Esencialmente, la evolución de las tecnologías de la información y

[30] Lucas Murillo de la Cueva, "La protección de los datos de carácter personal en el horizonte de 2010", 133.
[31] Ibíd., 134.
[32] Ibíd., 140.

comunicación; y los procesos de integración comercial, que exigen de los sistemas jurídicos adoptar los mecanismos propios de regulación y tutela necesarios para la protección de la información personal.

En América Latina, la protección de datos surge como "una necesidad resultado de la explosión tecnológica, pero inevitablemente todos los procesos legislativos en la región han sufrido los avatares de una fuerte carga histórica y de la presión de los intereses económicos en la generación de bases de datos"[33]. Precisamente, la Corte Constitucional de Ecuador –en adelante CCE–, ha resaltado que el *habeas data* constituye una garantía, que nace con el desarrollo tecnológico, para ejercer unas facultades de control sobre la información de carácter personal, tanto en el ámbito público como en el privado[34]. Sobre esta base, la protección de la información de carácter personal ha transitado, desde la incorporación del *habeas data,* en los textos constitucionales latinoamericanos, hasta la promulgación de Leyes generales y sectoriales sustentadas, principalmente, en el modelo europeo[35].

Como hemos mencionado, el reconocimiento del derecho a la protección de datos, dentro del marco jurídico de los Estados, es consecuencia de los procesos de integración comercial, que obligan a los sistemas jurídicos a articular una legislación acorde a estándares internacionales, principalmente, provenientes de la Unión Europea. Con referencia a este aspecto, apuntamos que, "esta aproximación de los países iberoamericanos al modelo europeo de protección de datos personales está siendo premiado con la declaración por parte de la Comisión Europea de que estos países garantizan un nivel adecuado de protección"[36].

---

[33] Carlos Gregorio, "Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina", en Raúl Márquez Romero (coord.), *Transparentar al Estado: La experiencia mexicana de acceso a la información,* (México: Instituto de Investigaciones Jurídicas, 2005), 310.

[34] Véase el Registro Oficial 18 de 3 de septiembre del 2009 –Caso signado con el Nro. 14-9-EP–.

[35] Así también la CCE ha destacado que el *habeas data* "es una institución reciente, en relación a otras como el hábeas corpus que tiene muchas décadas de existencia, pero va generalizándose en el nuevo Derecho Constitucional Latinoamericano, cobrando nuevas dimensiones con la expansión de la informática, los sistemas de Internet y conjugando con aquellos derechos que, de modo directo o mediato sirven para tutelar o garantizar esos derechos inalienables y universales, como son aquellos ligados a la dignidad del ser humano". Véase el Registro Oficial Suplemento 281 de 9 de marzo del 2001 –Caso signado con el Nro. 39-2000-HD–.

[36] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 182.

Instrumentos jurídicos regionales de reciente promulgación, como la Guía legislativa de la OEA sobre los "Principios de privacidad y protección de datos personales" y los "Estándares de protección de datos personales para los Estados Iberoamericanos" coinciden en que la falta de armonización y unidad en las legislaciones compromete, seriamente, la protección integral de este derecho fundamental. Respecto a esto, las principales consideraciones, por las cuales se promueven estos instrumentos, se encuentran enmarcadas en los nuevos desafíos que plantea la evolución tecnológica y, desde luego, en las dificultades y/o limitaciones que en los procesos de integración comercial puede ocasionar la ausencia de niveles adecuados para la garantía del derecho a la protección de datos[37].

Por ello, en el supuesto de una regulación que no enfrente a estas exigencias, advertimos que "el conflicto radica en que una protección así, parece insostenible con las demandas de desarrollo económico; puesto que las economías latinoamericanas necesitan agilizar el comercio"[38]. Así, encontrándose las economías latinoamericanas en procesos de crecimiento y desarrollo que conllevan la integración comercial, es imprescindible posibilitar que, en el tratamiento de la información personal, la legislación de protección datos cumpla con las condiciones y presupuestos que exige este derecho fundamental, en el ámbito internacional.

En cualquier caso, como apunta Puccinelli:

> En esa labor de contención, en el plano jurídico se generaron nuevas herramientas, en concreto y fundamentalmente puestas a disposición a partir de dos fenómenos principales: la creación de un nuevo derecho con contenidos diferenciales respecto de otros de los que puede aparecer como una mera escisión (el derecho a la protección de datos) y la formulación de reglas específicas tendientes a la protección de las personas frente a los abusos de este nuevo poder. Ambos aspectos, en definitiva, provocaron acaso el nacimiento de una nueva rama del derecho, el derecho de la protección de datos[39].

[37] Véase, especialmente, las notas introductorias de los Principios de privacidad y protección de datos personales de la OEA; y los considerandos 9, 16 y 21 de los Estándares de protección de datos personales para los Estados Iberoamericanos".

[38] Gregorio, "Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina", 325.

[39] Oscar Puccinelli, "Tipos y subtipos de *habeas data* en América Latina", *Editorial Astrea*, Nro. 4 (2004), 1-20 Consultado en Base de Datos: Vlex.com: ‹https://app.vlex.com/#WW/vid/26542396/graphical_version›.

En el inicio de este proceso de desarrollo tecnológico, en Latinoamérica, se configuró la necesidad de hacer frente a este fenómeno, desde el ámbito jurídico con el objeto de adoptar un modelo que beneficie, por un lado, los procesos comerciales pero que, en todo caso, legitime el intercambio de información, a través, del derecho a la protección de datos. Así, según Puccinelli, el primer país americano en contemplar, desde el marco constitucional el amparo del derecho a la protección de datos de carácter personal fue Guatemala en la Constitución de 1985, seguido de Nicaragua en 1987. Brasil, en 1988, incorpora en su Constitución la protección de este derecho como una garantía, mediante el *habeas data,* a pesar de no considerarlo, propiamente, un derecho vinculado al control del tratamiento de los datos. Finalmente, la protección de la información personal se plasmó en el ámbito constitucional en Colombia en 1991; Paraguay en 1992; Perú en 1993; Argentina en 1994; Ecuador en 1996; y Venezuela en 1999[40].

Esta suerte de dispersión normativa, desde el ámbito constitucional, ha supuesto que, en Ecuador, por ejemplo, exista una falta de procedimientos sectoriales internos, que evidencian la necesidad de contar con un modelo jurídico homogéneo, el cual propenda a la protección efectiva de la información de carácter personal, no solamente en el ámbito local sino también internacional. Un ejemplo de esto último, es la regulación de la transferencia internacional de datos personales que "pone de manifiesto la necesidad de incluir a la armonización legislativa como un aspecto de relevancia no sólo para el fortalecimiento de los propios sistemas de protección de datos, sino también con miras en el desarrollo de la economía digital"[41].

Si la intención es armonizar el marco de protección y acentuar los procesos de desarrollo económico y el crecimiento del comercio, la protección de datos en el mundo moderno "sólo es posible si se consensuan unas exigencias homogéneas de privacidad, que superen las discrepancias existentes –por no decir los

[40] Cfr. Puccinelli, "Tipos y subtipos de *habeas data* en América Latina", 4.
[41] Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", 27.

desequilibrios– entre la Unión Europea, Estados Unidos y el ámbito Asia-Pacífico y ofrezcan seguridad jurídica a todos los agentes"[42].

En este contexto, cuando la naturaleza jurídica de una figura legal no resulta clara y tiende a ser diversa, producto de procesos de integración económicos, políticos o sociales, es preciso recurrir a las fuentes del derecho o al espíritu mismo en que se origina su fundamento, a condición de la variación del lenguaje por la esfera social en la que se aplica. En este objetivo, la doctrina especializada nos permitirá comprender los aspectos más esenciales del derecho fundamental a la protección de datos personales, atendiendo las principales novedades que plantea el control de la información personal. Precisamente, mediante la teoría tridimensional del derecho se abordarán las condiciones que contempla este derecho, como hecho, valor y norma.

## 4. El derecho fundamental a la protección de datos personales como hecho, valor y norma

Considerando que, "en estos tiempos de globalización indetenible, conviene hacer de vez en vez un alto en el camino y preguntarse qué está ocurriendo con nuestra latinoamericanidad en su mestizaje constitutivo europeo-americano y hacia donde nos encaminamos"[43]; reiteramos que:

> En este contexto complejo y de cambio vertiginoso confluyen el derecho al desarrollo económico y tecnológico de los pueblos, la libre iniciativa, y la libertad de competencia, pero también el derecho a la libertad de expresión, de comunicación y de opinión; el derecho a la inviolabilidad de la intimidad, de la vida privada, del honor y de la imagen; el derecho de acceso a la información; el derecho la privacidad y de la autodeterminación informativa[44].

El derecho fundamental a la protección de datos personales se caracteriza, por ser un derecho global. A partir, del fenómeno de la globalización, enfrenta una serie de riesgos que afectan, principalmente, a la capacidad de control de la información por

[42] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 183.
[43] José Ledesma Uribe, "En torno a la teoría tridimensional del derecho de Miguel Reale", *Anuario del Departamento de Derecho de la Universidad Iberoamericana*, Nro. 33 (2003): 189-198.
[44] Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", 17.

parte de los titulares de datos personales. Así, comprendemos que el problema no se encuentra en adoptar modelos de regulación que, internacionalmente, gozan de reconocimiento o niveles adecuados de protección. En todo caso, hay que asumir que "la protección de datos personales, si es importante dentro del Estado nación, lo es especialmente teniendo en cuenta un mundo globalizado"[45]. La principal dificultad, en el ámbito regional y nacional, se presenta cuando los marcos jurídicos de los Estados tienden a adoptar un modelo carente de unidad y armonía con relación a los niveles, principios y procedimientos que la comunidad internacional tiene, claramente, definidos, frente a la tutela del derecho a la protección de datos.

En la búsqueda de ese equilibrio y armonización legislativa que precisa este derecho fundamental, "el asunto no es únicamente tema de nacionalidades, es tópico que por ende, atañe también al Derecho, a su forma de conocerlo, concebirlo, hacerlo operar y vivirlo"[46]. Como señala Bobbio, "ciertas exigencias nacen sólo cuando nacen ciertas necesidades. Nuevas necesidades nacen en relación al cambio de las condiciones sociales, y cuando el desarrollo técnico permite satisfacerlas"[47].

Como sabemos, el derecho a la protección de datos personales plantea ciertas exigencias, como resultado de la necesidad de integración económica de los Estados, en una sociedad globalizada y caracterizada por el desarrollo tecnológico. Así, apegados a los postulados de la teoría tridimensional del derecho intentaremos "facilitar la comprensión de las instituciones jurídicas, mostrándolas en su interacción con la conducta subjetiva, el valor y la norma"[48]. En este caso, lo haremos en relación a la institución jurídica que comprende el derecho a la protección de datos.

[45] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 170.
[46] Ledesma Uribe, "En torno a la teoría tridimensional del derecho de Miguel Reale", 189.
[47] Norberto Bobbio, *El tiempo de los derechos humanos,* (Madrid, Editorial Sistema. Fundación Sistema, 1991), 19.
[48] Martha Olivia Cano-Nava, "Modelo epistemológico de la teoría tridimensional del derecho", *Revista de Ciencias Sociales: Convergencia*, Nro. 57 (2011): 209-228.

Según la teoría tridimensional, la protección de datos personales asume "la dimensión fenomenológica, esto es, el hecho desencadenante de la necesidad de protección jurídica (…) la perspectiva ética, axiológica, en suma, el valor, en nuestro caso la intimidad (…) por último la perspectiva jurídica, la norma"[49]. No obstante, aclaramos que, desde la perspectiva ética y/o axiológica el valor no se encuentra representado, únicamente, por la intimidad; por cuanto este derecho fundamental se concibe como un instituto de garantía de otros derechos que, distintos al derecho a la intimidad, pretende conciliar el uso de las tecnologías con el respeto a la dignidad humana.

En la actualidad, abordar el derecho a la protección de datos personales, desde la perspectiva de la teoría tridimensional, no parece una idea tan alejada de la realidad puesto que, –como señala Lucas Murillo de la Cueva–, "es cuestión, sencillamente, de seguir tomando en serio este derecho fundamental para garantizar que, junto a los restantes constitucionalmente reconocidos, suministre a las personas los medios jurídicos que precisan para asegurar la satisfacción de sus necesidades básicas"[50].

Desde este punto de vista, la teoría tridimensional se entiende como:

> El resultado de la interacción dinámica de la vida humana social, valores y normas, es decir, la regulación valiosa y obligatoria de la vida humana social. El derecho cumple así una doble función: protege la libertad de cada ser humano dentro del contexto social y asegura que dicha interrelación personal no atente contra el interés social y el bien común[51].

Admitiendo que esta teoría concibe una realidad, desde la posición normativa, factual y ética, al momento de establecer una visión integral del derecho; el estudio de la protección de datos personales implica que "la correlación entre dichos tres elementos es funcional y dialéctica -dada la implicación o polaridad- existente entre hecho y valor de cuya tensión resulta el momento normativo"[52].

---

[49] Rodríguez Pérez, "Tridimensionalismo jurídico y protección de datos personales frente a su tratamiento automatizado", 4.
[50] Lucas Murillo de la Cueva, "La protección de los datos de carácter personal en el horizonte de 2010", 142.
[51] Cano-Nava, "Modelo epistemológico de la teoría tridimensional del derecho", 215.
[52] Miguel Reale, *Teoría Tridimensional del Derecho*, (Madrid: Editorial Tecnos, 1997), 72.

En este plano, y con referencia al modelo europeo, mencionamos que, en la Unión Europea, desde el año 2000 "se abre una nueva etapa, en la que nos encontramos, que se basa en la consideración de la protección de datos de carácter personal como un verdadero Derecho fundamental autónomo e independiente del Derecho a la intimidad"[53]. En efecto, el 7 de diciembre del 2000, el Parlamento Europeo, el Consejo y la Comisión proclamaron la Carta de los Derechos Fundamentales de la Unión Europea. La Carta reconoce a la protección de datos de carácter personal como un derecho autónomo –art. 8–, respecto al derecho a la vida privada y familiar –art. 7–. Hay que anotar, además, la importancia del Tratado de Lisboa, por cuanto este instrumento asigna un valor jurídico a la Carta de Derechos de la Unión Europea. En este sentido, este Tratado "refuerza las bases jurídicas específicas para que la Unión Europea apruebe una normativa sobre protección de datos personales aplicable a todos los ámbitos"[54]. En la actualidad, esta iniciativa desembocó en la aprobación de un nuevo marco europeo sobre protección de datos y que se encuentra materializado en el RGPD, y en la Directiva 95/46/CE relativa al tercer pilar. Este marco normativo está orientado a la protección de los datos personales como resultado de nuevos contextos que se derivan por la evolución de las tecnologías de la información y comunicación[55].

Ahora bien, particular importancia tiene el carácter autónomo, por el cual el derecho a la protección de datos personales se distingue del derecho a la intimidad. En este caso, apuntamos que:

> El derecho fundamental a la protección de datos se encuentra muy relacionado con el derecho a la intimidad, estando incluido dentro del precepto constitucional que reconoce y proclama distintos derechos relativos a la privacidad de las personas. Pero, al mismo tiempo, es un derecho autónomo a controlar la propia información personal (sea íntima o no lo sea), un derecho general frente a los riesgos para los derechos de la personalidad que pueden

[53] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 93.
[54] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 34.
[55] El RGPD expresa que: "Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales" –Considerando 7–.

> suponer el tratamiento de datos personales y, por tanto, una garantía de instituto de otros derechos fundamentales[56].

Refiriéndonos a Ecuador, por ejemplo, confrontamos esta distinción en la Constitución de 2008, ya que el derecho a la protección de datos personales y el derecho a la intimidad personal y familiar se reconocen y garantizan por separado[57]. En el caso de España existen referentes jurisprudenciales del Tribunal Constitucional, que marcan una separación conceptual entre la intimidad y el derecho a la protección de datos como un derecho autónomo e independiente. Al respecto, resaltamos la STC 292/2000, la cual señala que:

> La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 C.E.), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es así derecho a controlar el uso de los mismos datos insertos en un programa informático (*habeas data*) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención[58].

En este sentido, apreciamos que:

> El derecho a la intimidad protege tradicionalmente los datos íntimos de la persona que, por el hecho de serlo, deben estar excluidos del conocimiento de los demás; en cambio, el derecho fundamental a la protección de datos personales tutela cualquier dato, sean o no íntimo. Los datos que son de conocimiento público no dejan, por ello, de pertenecer al poder de disposición de la persona. Este derecho fundamental no protege únicamente la información privada del individuo, sino cualquier información referida a una persona; incluso la información conocida por toda la sociedad[59].

En todo caso, a pesar de considerarse a la protección de datos personales como un derecho autónomo, no debe olvidarse que en la práctica este derecho permite salvaguardar, entre otros derechos, también el derecho a la intimidad en su calidad de instituto de garantía; toda vez que, tutela, especialmente, los datos íntimos. De este modo, se consagra como "un instituto de garantía de otros derechos

[56] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 75.
[57] En la Constitución de la República del Ecuador de 2008, el derecho a la intimidad personal y familiar se regula por separado en el art. 66.20, en relación con el derecho a la protección de datos de carácter personal contemplado en el art. 66.19.
[58] Véase la Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1463/2000. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332.
[59] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 133.

fundamentales, en especial del derecho a la intimidad, pero no sólo de este derecho"[60].

Por lo que se refiere a la perspectiva jurídica, en el caso de Ecuador, el derecho fundamental a la protección de datos personales se encuentra contemplado en la Constitución, en el art. 66.19. Así, como un derecho de libertad, se reconoce y garantiza:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley.

Según este reconocimiento constitucional, el derecho a la protección de datos se caracteriza por: a) garantizar el acceso y la decisión sobre información y datos de este carácter; b) estimar mecanismos de protección, mediante el *habeas data*; y c) establecer condiciones, dentro del tratamiento de la información, reguladas por el mandato legal o, en virtud, del consentimiento que debe prestar el titular de los datos personales. En este contexto, sin el ánimo de ser concluyentes, entendemos que el concepto de protección de datos personales comprende: la regulación del poder de disposición y control de la información de carácter personal y los mecanismos de control o garantías que se generan a partir del tratamiento por parte de terceros.

Hasta aquí, hemos insistido en la necesidad de revisar las causas que motivaron el surgimiento del derecho a la protección de datos, a partir de las condiciones que plantea la teoría tridimensional del derecho. Una primera conclusión, sobre este respecto, es que el hecho económico, político y social obliga a replantear los modelos de regulación en la materia, tanto por los procesos de integración económica, como por la evolución de las tecnologías de la información y comunicación[61]. En este orden, advertimos que:

---

[60] Ibíd., 69.

[61] Con referencia a este aspecto, el RGPD refiere que la "integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos de datos personales" –Considerando 5–. Así también establece que la "rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos

> El movimiento de personas, de mercancías y de capitales implica también el intercambio de información personal lo que obliga a tener unos estándares comunes de protección de datos personales que permitan este intercambio de información (…) Al mismo tiempo, una legislación estrictamente nacional de protección de datos personales no es efectiva ya que los tratamientos de datos personales se desarrollan por Internet a través de redes internacionales cuyo servidor informático se encuentra en un tercer país[62].

Ahora bien, desde la perspectiva ética, axiológica, valor y/o bienes jurídicos que comprende el derecho a la protección de datos, consideramos que éste se constituye como un derecho autónomo, destinado a tutelar el control de la información personal, frente al tratamiento de terceros; y que, en todo caso, se concibe como un instituto de garantía de otros derechos fundamentales, respecto a los riesgos que supone la disposición ilegítima en una sociedad globalizada[63].

## 5. Reflexiones desde la teoría del Derecho Constitucional

En la era de las tecnologías de la información y comunicación, reflexionar sobre la naturaleza de nuevos derechos adquiere especial significación. “En el período en que vivimos, marcado por la globalización, las sociedades de individuos no pueden adaptarse tanto al ámbito de las constituciones estatales, dado que responden a

personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales” –Considerando 6–.

[62] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 170.

[63] Sobre esta consideración, los Estándares de protección de datos personales de 2017 destacan que “el derecho a la protección de datos personales se ha conceptualizado en algunos países Iberoamericanos, legislativamente o jurisprudencialmente, como un derecho de naturaleza distinta a los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y otros derechos similares, que en su conjunto garantizan el libre desarrollo de la personalidad de la persona física, hasta conformarse en un derecho autónomo, con características y dinámica propias, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona física con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana” –Considerando 2–.

una serie de reglas supraconstitucionales, de carácter global y no local"[64]. Esta apreciación se ve más acentuada cuando se hace referencia a la teoría jurídica del neoconstitucionalismo, la cual promueve el desarrollo de nuevos derechos.

Siendo una de las características de los sistema jurídicos de la región que los jueces ordinarios "antes solo preocupados de dirimir los conflictos jurídicos en sus respectivas áreas de especialidad, hoy día se han convertido en jueces constitucionales, mediante el ejercicio de las competencias respecto de las garantías jurisdiccionales de los derechos"[65]; desde la teoría constitucional, el derecho a la protección de datos personales plantea ciertas condiciones, que aseguren, en suma, el principio de seguridad jurídica de los ciudadanos.

> Por tanto, en la actualidad sigue siendo útil releer la libertad de información como derecho a ser informado, así como a informar, la libertad de comunicación, la libertad de asociación, la libertad de reunión, la libertad de iniciativa económica privada y las libertades políticas; todo ello, a la luz del desarrollo de la tecnología informática y con el fin de determinar así las formas de protección de las nuevas situaciones jurídicas subjetivas[66].

El neoconstitucionalismo supone que el Estado y los particulares ajusten sus decisiones, siguiendo el mandato constitucional. En este sentido, es la Constitución "la que delimita los alcances de los derechos; pues hay que considerar (como deducción de la tesis neoconstitucionalista de Luis Prieto Sanchís), que viene instituida como norma material de la cual se busca su garantía"[67]. Así, a la luz de la teoría neoconstitucional, será importante abordar la defensa, protección y garantía del derecho a la protección de datos personales, mediante un estudio pormenorizado de los derechos humanos y la transformación del "Estado de

[64] Tommaso Edoardo Frosini, "Nuevas tecnologías y constitucionalismo", *Revista Derecho del Estado*, Nro. 15 (2003): 29-43.
[65] Juan Montaña y Patricio Pazmiño, "Algunas consideraciones acerca del nuevo modelo constitucional ecuatoriano", en Jorge Benavides Ordóñez y Jhoel Escudero Soliz (coord.), *Manual de justicia constitucional ecuatoriana, (*Quito-Ecuador: Centro de Estudios y Difusión del Derecho Constitucional, 2013), 42.
[66] Frosini, "Nuevas tecnologías y constitucionalismo", 30.
[67] José Fernando Villacrés, "La aplicación directa de la Constitución frente al prevaricato en Ecuador", en Jorge Benavides Ordóñez y Jhoel Escudero Soliz (coord.), *Manual de justicia constitucional ecuatoriana (*Quito-Ecuador: Centro de Estudios y Difusión del Derecho Constitucional, 2013), 350.

Derecho", hacia el actual paradigma del "Estado constitucional de derechos y justicia"[68].

En primer término, destacamos que:

> En el análisis de la libertad informática bajo el prisma del derecho constitucional, y volviendo la mirada a través de algunas cartas constitucionales recientes, se puede observar cómo la elaboración de la normativa constitucional ha tenido en cuenta el desarrollo tecnológico informático, y por tanto, se ha procedido a redactar normas constitucionales de las cuales puede deducirse el principio de libertad informática en sentido activo y pasivo[69].

Al instituirse como una teoría jurídico-constitucional que, requiere el discernimiento de varios tópicos jurídicos, –entiéndase por aquellos: la relación constitución, derechos fundamentales, normas, principios, ponderación, entre otros–; analizaremos el origen del derecho a la protección de datos personales, desde el neoconstitucionalismo andino con un enfoque hacia los derechos humanos[70].

### 5.1 Aproximación al concepto neoconstitucional

Con el objeto de comprender el contenido del concepto neoconstitucionalismo, precisamos tomar en cuenta las bases que sustentan esta teoría. Es decir, analizar la constitucionalización del derecho. Para Riccardo Guastini, la constitucionalización del derecho produce en el aparato estatal un cambio y desarrollo jurídico sustentado, en por lo menos siete condiciones, a saber: 1. Rigidez de la constitución; 2. Control de la constitucionalidad de las Leyes; 3. Carácter políticamente vinculante de la constitución; 4. Interpretación de la norma constitucional; 5. Aplicación primaria de las normas constitucionales por los jueces;

---

[68] La Constitución de 2008 establece que "El Ecuador es un Estado constitucional de derechos y justicia" –art. 1–. Al respecto, la CCE precisa que "aquello significa que el centro del Estado, es el ser humano, que toda su actividad debe encaminarse a buscar el bienestar de sus habitantes a través del respeto de todos los derechos consagrados no sólo en la Constitución, sino demás Leyes e instrumentos internacionales, para lo cual, en caso de vulneración, la misma Constitución ha implementado las garantías jurisdiccionales". Véase Resolución de la Corte Constitucional 344, Registro Oficial Suplemento 889 de 24 de noviembre del 2016.

[69] Frosini, "Nuevas tecnologías y constitucionalismo", 32.

[70] Como explica Ramiro Ávila Santamaría, el neoconstitucionalismo andino surge como una teoría jurídica, inconforme con la teoría tradicional y con la realidad actual, que busca enfatizar la protección y regulación eficaz de los derechos fundamentales a partir de siete instituciones: la plurinacionalidad, *la pachamama, el sumak kawsay*, la democracia comunitaria, la justicia indígena y la interculturalidad.

6. Relación del caso con la Ley ordinaria; y 7. Influencia directa de la constitución en las relaciones políticas[71].

El debate se centra en la eficacia de la norma constitucional en la práctica, lo cual se vincula con la efectiva tutela de los derechos fundamentales. Si bien, en el constitucionalismo contemporáneo se proclama la justiciabilidad de los derechos fundamentales; este presupuesto en la praxis no se cumple. Por ello, con el reconocimiento y la garantía constitucional del derecho a la protección de datos no es suficiente debido a que, "por ejemplo: los altos costos transaccionales, la ineficiencia en la prevención del incumplimiento, la falta de *stare decisis* de las decisiones judiciales –ya que, salvo contadas excepciones–, sólo aplican al caso sujeto a decisión judicial"[72].

Es importante dilucidar en qué momento resulta equívoco el fin u objeto de los derechos fundamentales, bien en la teoría, a través, de sus fundamentos, o en la práctica, mediante las condiciones que el Estado prevé para su plena satisfacción. En todo caso, precisamos que "no puede considerarse superado completamente el ejercicio hermenéutico de querer aplicar las libertades constitucionales estatales a los fenómenos de las tecnologías informáticas"[73]. El desafío que plantea este nuevo paradigma constitucional admite que la garantía de los derechos fundamentales supone que el Estado, a través, de un sistema de garantías introduzca, en el ámbito político, el desplazamiento del poder legislativo hacia el poder judicial, en virtud de la observancia de ciertas condiciones de constitucionalización.

Por otra parte, Paolo Comanducci distingue tres formas de neoconstitucionalismo: el teórico, el ideológico y el metodológico[74]. El teórico, que implica la representación material en el Estado del neoconstitucionalismo, es decir, el proceso de reforma y positivización de los derechos fundamentales en el sistema jurídico sustentado en

[71] Riccardo Guastini, "La 'constitucionalización' del ordenamiento jurídico: el caso italiano", en Miguel Carbonell (coord.), *Neoconstitucionalismo* (Madrid: Editorial Trotta, 2003).
[72] Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", 22.
[73] Frosini, "Nuevas tecnologías y constitucionalismo", 30.
[74] Cfr. Paolo Comanducci, "Formas de Neoconstitucionalismo: un análisis metateórico", en Miguel Carbonell (coord.), Neoconstitucionalismo (Madrid: Editorial Trotta, 2003), 83.

un proceso, eminentemente, normativo; el ideológico, que establece como premisa la garantía de los derechos, lo que a diferencia del modelo anterior, no se concentra en describir el proceso de constitucionalización, sino que, se apoya en la defensa y ampliación de mecanismos jurídicos para la garantía de los derechos fundamentales, el cual se instituye, desde el ente legislativo y judicial; y finalmente, el metodológico encaminado a establecer una posición adecuada sobre la existencia de una correlación entre el derecho y la moral.

Independientemente, de los modelos anotados, sugerimos que según la teoría neoconstitucional "uno de los aspectos más destacados de discusión sobre los derechos fundamentales es la posibilidad que tiene el Estado constitucional para responder adecuadamente (es decir, a través de los medios ordinarios de defensa que ya conocemos)"[75]. Como se sabe, el neoconstitucionalismo supone el reconocimiento y garantía de los derechos consagrados –tanto, en la Constitución, como en los instrumentos internacionales– y, por tanto, exige su aplicación en el poder judicial. Así, en el ámbito judicial, frente al "escenario de la tecnología informática y su impacto sobre las libertades tradicionales del ciudadano, el juez constitucional debe saber recuperar las libertades constitucionales actualizándolas a través de la vía interpretativa y situándolas en el prisma del derecho de la libertad informática"[76].

Ahora bien, en el caso de Ecuador, entendemos que:

> La significación de ser un Estado constitucional de derechos es una superación a nuestra construcción como un Estado social de derecho. De aquí se desprende una innovación en la propia estructura de la legalidad, que es quizá la conquista más importante del derecho contemporáneo: la regulación jurídica del derecho positivo mismo, no solo en cuanto a las formas de producción sino también por los que se refiere a los contenidos producidos. Así ha nacido el modelo "garantista" que proclama la invalidez del derecho ilegítimo[77].

Por tanto, cuando la Constitución caracteriza al Estado ecuatoriano como "constitucional de derechos y justicia" se establece que "el máximo deber del estado

[75] Miguel Carbonell, "Prologo", en Ramiro Ávila Santamaría, *Neoconstitucionalismo y Sociedad,* (Quito-Ecuador: Ministerio de Justicia y Derechos Humanos, 2008), 11.
[76] Frosini, "Nuevas tecnologías y constitucionalismo", 37.
[77] Jorge Zavala Egas, *Derecho Constitucional, Neoconstitucionalismo y Argumentación Jurídica*, (Quito-Ecuador: Edilex S.A. Editores, 2010), 141.

es garantizar los derechos, está obligando a toda autoridad pública a que respete derechos, cualquiera que fuese el acto jurídico mediante el cual se manifieste: Ley, reglamento, sentencia, plan nacional"[78].

Al respecto, la CCE aclara que:

> Hoy en día vivimos un constitucionalismo contemporáneo o neoconstitucionalismo que genera el desarrollo de una nueva teoría jurídica, muy distinta al positivismo legalista antiguo, que tienen como características resaltadas, las siguientes: 1) Es un Derecho más de principios que de reglas; 2) Mayor utilización del principio de ponderación; 3) Una plenitud constitucional que llena al detalle el ordenamiento jurídico, dejando menos ámbito para la Ley; 4) Poder del juez, para la determinación de derechos, en lugar de la antigua exclusividad del legislador para desarrollarlos[79].

Evidenciamos un cambio de estructura del sistema jurídico constitucional, puesto que, el modelo neoconstitucional supone la amplia consagración de los derechos fundamentales. Por tanto, introduce la implantación de límites en el ejercicio de las Administraciones Públicas. Una de esas limitaciones es la arbitrariedad en las decisiones, lo cual obliga a que los poderes públicos apliquen de manera directa e inmediata –como una regla de decisión– los derechos y garantías reconocidos en la Constitución y los instrumentos internacionales. En este sentido, la CCE agrega que "la concepción del Estado garantista es la del Estado constitucional de derechos, es decir, aquel que se construye sobre los derechos fundamentales de la persona y en el rechazo al ejercicio del poder arbitrario"[80].

Esta transformación es considerada por la doctrina latinoamericana como una tendencia que responde al neoconstitucionalismo andino. Así, el modelo de Ecuador –definido como un Estado constitucional de derechos y justicia– se afirma en el modelo ideológico que describe Paolo Comanducci, cuya base implica la determinación de mecanismos garantistas para hacer realidad, en la práctica, los derechos fundamentales, pasando del discurso legal a la praxis de los derechos; de

[78] Ramiro Ávila Santamaría, *El Neoconstitucionalismo andino,* (Quito-Ecuador, Universidad Andina Simón Bolívar, 2016), 61.
[79] Véase Resolución de la Corte Constitucional 344, Registro Oficial Suplemento 889 de 24 de noviembre de 2016.
[80] Ibíd.

la exclusión a la inclusión; de la intolerancia y negación, a la inclusión y respeto a la diversidad y pluralidad.

Como analizaremos más adelante, el surgimiento del derecho fundamental a la protección de datos, a partir, de la teoría neoconstitucional supone una de las más importantes cuestiones que desarrolló la Reforma Constitucional de 2008. Desde luego, la base se centró, en la formulación de derechos fundamentales innovadores que –contenidos en instrumentos internacionales–, protegen la información de carácter personal, y garantizan su aplicación de forma directa e inmediata, por cualquier servidor público, administrativo o judicial.

### 5.2 Derivación del derecho a la protección de datos personales según la teoría de los derechos humanos

A lo largo del estudio que pretende fundamentar los derechos humanos, encontramos en primer lugar la corriente iusnaturalista. Esta corriente ha planteado varios problemas teóricos referente a la aceptación de sus principios, por cuanto, según la doctrina iusnaturalista, se asume que los derechos naturales de las personas "en cuanto dictados por la naturaleza y no impuestos por una autoridad externa, son anteriores al Estado y constituyen, por tanto, para la autoridad política un límite insuperable"[81].

Desde esta perspectiva, Bobbio considera que:

> La doctrina de los derechos del hombre ha nacido de la doctrina iusnaturalista, la cual, para justificar la existencia de derechos pertenecientes al hombre en cuanto tal, independientemente del Estado, partía de la hipótesis del estado de naturaleza, donde los derechos del hombre eran pocos y esenciales[82].

Tomando en consideración que el Derecho Natural constituye el ordenamiento o las disposiciones que proceden de las Leyes de la naturaleza, y que de éstas se desprenden los derechos que le corresponden al hombre, por su condición humana y propia hacia la naturaleza; el iusnaturalismo considera que los derechos que los

[81] Bobbio, *El tiempo de los derechos humanos,* 29.
[82] Ibíd., 119.

individuos ejercen en la sociedad, en sus relaciones interpersonales, proceden de las Leyes de la naturaleza, antes que de un ordenamiento jurídico positivo.

El proceso de fundamentación de los derechos humanos, basados en la naturaleza humana, supone que la defensa y la garantía de los derechos no deviene de la imposición del Estado o de los ordenamientos jurídicos. Así, se advierte que "la historia universal lo ha sido más de la ignorancia que de protección de los derechos de los seres humanos frente al ejercicio del poder. El reconocimiento universal de los derechos humanos como inherentes a la persona es un fenómeno más bien reciente"[83]. Esta pugna de considerar si los derechos humanos encuentran su fundamento en Leyes que proceden de normas superiores, o a su vez en ordenamientos jurídicos positivos, resulta un tanto ambigua y difícil de despejar, al momento de determinar la base sobre la cual se pretenda exigir su cumplimiento, desde el Estado o de otras personas que, en similares circunstancias, procuran hacer valer sus derechos.

Otra corriente que ha marcado el proceso de fundamentación de los derechos humanos, sustentados en la dignidad humana, es la iuspositivista. Desde esta teoría, los derechos de las personas –sobre la base de los ordenamientos jurídicos positivos– nacen de las limitaciones que el Estado se impone a sí mismo, y a todas las personas, en su deber de garantizar y respetar los derechos fundamentales.

Como agrega Bobbio:

> Para el positivismo jurídico los pretendidos derechos naturales no son sino derechos públicos subjetivos, «derechos reflejos» del poder del Estado, que no constituyen un límite al poder de éste, anteriores al nacimiento del mismo Estado, sino que son una consecuencia, al menos en la célebre y conocida doctrina de Jellinek, de la limitación que el Estado se impone a sí mismo[84].

Frente a esta teoría, la CCE advierte que, en el Estado constitucional de derechos:

> El legalismo no es suficiente para considerar frenado o limitado al poder legislativo que, libérrimo en cuanto a dotar de cualquier contenido a las Leyes, puede ejercerse, junto a su

[83] Pedro Nikken, "Sobre el concepto de Derechos Humanos", en Instituto Interamericano de Derechos Humanos, *Seminario de Derechos Humanos,* (San José – Costa Rica: IIDH, 1997), 19.
[84] Bobbio, *El tiempo de los derechos humanos,* 170.

> aplicación automática por parte de los operadores de la justicia, en forma autoritaria y despótica. El Estado que asume el garantismo, en cambio, es el que vincula los derechos fundamentales consagrados en la Constitución con todos los poderes públicos[85].

Tanto desde, el iusnaturalismo como el iuspositivismo, el origen de los derechos se concibe desde los fundamentos de la dignidad humana. Este reconocimiento representa la máxima garantía, frente al ejercicio del poder arbitrario. Por ello, hay que considerar que, aun cuando "la hipótesis del estado de naturaleza haya sido ya abandonada, las primeras palabras con las que comienza la Declaración Universal de Derechos Humanos mantienen un preciso eco de ella: «Todos los hombres nacen libres e iguales en dignidad y derechos.»"[86]. En este sentido, en materia de protección de datos, precisamos que "quien trata datos personales trata datos ajenos, no propios, que debe utilizar con estricto respeto a los derechos del interesado. Esta construcción nos reconduce al respeto de la dignidad de la persona, base fundamental de la protección de datos"[87].

Dentro de la teoría del neoconstitucionalismo andino es muy recurrente fundamentar el respeto y garantía de los derechos, sobre la base de la dignidad humana. Como expone Ávila Santamaría, la calificación del "estado de derechos", en las Constituciones se ha convertido en una articulación novedosa, donde el poder público y privado, se obliga al respeto de los derechos fundamentales reconocidos también en instrumentos internacionales de derechos humanos[88]. Así, como apunta la jurisprudencia en Ecuador, este respeto no persiste por sí solo. Requiere de la creación y establecimiento de procesos y mecanismos de tutela, que garanticen la directa e inmediata aplicación de las normas que regulen, en este caso, el tratamiento de la información personal. En todo caso, es necesario poner un especial énfasis en "la obligación que tienen las autoridades con facultad normativa,

[85] Véase Resolución de la Corte Constitucional 344, Registro Oficial Suplemento 889 de 24 de noviembre del 2016.
[86] Bobbio, *El tiempo de los derechos humanos,* 67.
[87] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 102.
[88] Cfr. Ávila Santamaría, *El Neoconstitucionalismo andino,* 57.

de respetar y garantizar el contenido material de la Constitución de la República y del corpus iuris internacional, recogido en el artículo 84 de la Constitución"[89].

Bajo las consideraciones que anteceden, al constituirse la protección de la información y de la vida privada de las personas, como derechos que tienen el carácter de universal, nuevos y/o de tercera generación, es preciso determinar su contenido y condiciones que posibiliten, en la práctica, la plenitud en su ejercicio[90].

## 6. Conceptualización de la protección de datos personales como un derecho fundamental

Las primeras revoluciones sociales independentistas, –francesa, norteamericana e iberoamericana–, configuran ciertos caracteres relacionados a los derechos humanos, fundamentados en los principios de libertad y la inexistencia de desigualdad social. Sobre todo, reconocen en la dignidad humana la base sobre la cual se asienta el respeto y la garantía de los derechos.

Desde esta perspectiva, apreciamos que:

> Es de esta forma que el tema de los derechos humanos ingresó al Derecho constitucional. Se trata en verdad, de un capitulo fundamental del Derecho constitucional, puesto que el reconocimiento de la intangibilidad de tales derechos implica limitaciones al alcance de las competencias del poder público. Desde el momento que se reconoce y garantiza en la Constitución que hay derechos del ser humano inherentes a su misma condición en consecuencia, se imponen límites al ejercicio del poder del Estado anteriores y superiores al poder del Estado, al cual le está vedado afectar el goce pleno de aquellos derechos[91].

El reconocimiento de los derechos fundamentales, sobre la base del respeto de la dignidad humana y de los límites que se imponen al poder público y privado, forma

---

[89] Véase Resolución de la Corte Constitucional 344, Registro Oficial Suplemento 889 de 24 de noviembre de 2016. En este orden, precisamos que el art. 84 de la Constitución señala que: "todo órgano con facultad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano".

[90] La Declaración Universal de los Derechos Humanos de 1948 refiere que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la Ley contra tales injerencias o ataques" –art.12–.

[91] Nikken, "Sobre el concepto de Derechos Humanos", 20.

parte de las características que desarrollan la construcción de un Estado constitucional de derechos y justicia. Siendo la dignidad humana el fundamento de las normas constitucionales, consideramos que el Estado constitucional de derechos y justicia supone que "cualquier poder, público o privado, debe ser limitado por los derechos constitucionales. Ejemplos abundan. Piénsese (…) en la discriminación en los arriendos o en el acceso a trabajos por cuestiones de origen nacional o color de piel"[92].

> Así pues, cualquiera sea el fundamento filosófico de la inherencia de los derechos humanos a la persona, el reconocimiento de la misma por el poder y haber quedado plasmada en instrumentos legales de protección en el ámbito doméstico y en el internacional, han sido el producto de un sostenido desarrollo histórico, dentro del cual las ideas, el sufrimiento de los pueblos, la movilización de la opinión pública y una determinación universal de la lucha por la dignidad humana, han ido forzando la voluntad política necesaria para consolidar una gran conquista de la humanidad, como es el reconocimiento universal de que toda persona tiene derechos por el mero hecho de serlo[93].

El actual Estado constitucional ecuatoriano se sostiene sobre un sistema jurídico que respeta, en todas sus dimensiones, la dignidad de las personas y las colectividades[94]. Esto supone, no solamente el reconocimiento de los derechos establecidos en la Constitución y en los instrumentos internacionales de derechos humanos[95], sino también en el respeto de los derechos que se derivan de la dignidad de las personas. De este modo, esta cláusula abierta "abre la posibilidad para que los derechos no reconocidos en la Constitución ni en instrumento

[92] Ávila Santamaría, *El Neoconstitucionalismo andino,* 55.
[93] Nikken, "Sobre el concepto de Derechos Humanos", 23.
[94] Es muy importante señalar que la Constitución ecuatoriana determina que: "El reconocimiento de los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos, no excluirá los demás derechos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, que sean necesarios para su pleno desenvolvimiento" –art. 11.7–.
[95] La CCE ha señalado que por normas ecuatorianas se entienden "aquellas que tienen vigencia y fuerza obligatoria en jurisdicción ecuatoriana, incluyendo aquellas establecidas en tratados y convenios internacionales, decisiones de organismos del sistema interamericano o universal de protección de derechos humanos, u otras fuentes de derecho, reconocidas en la Constitución de la República corno parte del ordenamiento jurídico del Ecuador". Cfr. Véase Resolución de la Corte Constitucional 184-18-SEP-CC. Caso Nro. 1692-12-EP.

internacional alguno, puedan ser justiciables. La referencia a la dignidad, sin duda, nos ofrece parámetros más objetivos para la determinación de derechos"[96].

En este sentido, los derechos fundamentales –incluida la protección de datos personales, como un derecho de libertad consagrado en la Constitución de Ecuador– tienen como fundamento el respeto de la dignidad de la persona. De esta forma, "es preciso destacar que el conocer y difundir qué supone el Derecho Fundamental a la Protección de Datos, resulta esencial para defender la libertad y dignidad"[97]. Además, a partir de los avances tecnológicos y procesos de integración económica, "se hace imprescindible reforzar el control sobre nuestros datos personales que, en último término, supone proteger nuestra dignidad personal frente a estos nuevos peligros"[98]. En todo caso, reflexionando sobre el instituto de garantía que comprende este derecho fundamental, la protección de las libertades relativas a la intimidad y a la propia imagen "han sido consideradas por la teoría jurídica tradicional como manifestaciones de los derechos de los derechos de la personalidad, y en el sistema actual de los derechos fundamentales como expresiones del valor de la dignidad humana"[99]. Naturalmente, "todos aquellos valores entroncan de forma directa con los principios de Democracia y Estado de Derecho, reconocidos como base de la Unión Europea en el mismo preámbulo de la Carta de los Derechos Fundamentales Europea"[100].

Por estas razones, "la protección de datos personales exige complementar los instrumentos de tutela internos con instrumentos de tutela que operen a nivel internacional. Las garantías establecidas en el espacio europeo constituyen un

[96] Ramiro Ávila Santamaría, *Los derechos y sus garantías. Ensayos críticos,* (Quito-Ecuador: Corte Constitucional para el Período de Transición, 2012) 87.
[97] María Nieves De la Serna Bilbao, "Las tecnologías de la información; derecho a la privacidad, tratamiento de datos y tercera edad", *Oñati Socio-Legal Series*, Nro. 8 (2011). ISSN 2079-5971.
[98] Mónica Arenas Ramiro, "*Unforgettable*: A propósito de la STJUE de 13 de mayo de 2014. Caso Costeja (*Google* Vs. AEPD)", *Revista Teoría y Realidad Constitucional*, Nro. 34 (2014):537-558.
[99] Antonio Pérez Luño, *Derechos humanos, Estado de Derecho y Constitución,* (Madrid: Tecnos, 2010), 323.
[100] De la Serna Bilbao, "Las tecnologías de la información; derecho a la privacidad, tratamiento de datos y tercera edad", 8.

evidente ejemplo de esta tendencia"[101]. Así, destacamos que el RGPD determina que "el tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad" –Considerando 4–. En este orden, la protección de datos se apoya en el principio de solidaridad como una fuente de las obligaciones, por cuanto "en sociedades complejas, la solidaridad es un principio que ayuda a cumplir las dimensiones prestacionales de la libertad, la igualdad sin discriminación, mediante las acciones afirmativas y hacer efectiva la dignidad"[102]. En la región se evidencia un significativo desarrollo de instrumentos internacionales, que posibilita la integración latinoamericana –en términos de armonizar, jurídicamente, la protección y tutela de este derecho fundamental–, a partir del respeto solidario de la dignidad humana.

Por ejemplo, la Guía legislativa de la OEA, sobre los "Principios de privacidad y protección de datos personales", significa un importante instrumento en la conceptualización del respeto del derecho a la protección de datos, como expresión de la dignidad humana. Como señala esta Guía legislativa:

> La finalidad de estos principios es instar a los Estados Miembros de la Organización a que adopten medidas para que se respete la privacidad, la reputación y la dignidad de las personas. Su propósito es servir de base para que los Estados Miembros consideren la posibilidad de formular y adoptar Leyes con objeto de proteger la información personal y los intereses en materia de privacidad de las personas en las Américas[103].

Ahora bien, en Ecuador, el derecho a la protección de datos tiene un reconocimiento constitucional que, conjuntamente, con la garantía del *habeas data* se articulan como un mecanismo de protección y tutela de la información de carácter personal. Por esto, asumiendo que en el derecho comparado, por ejemplo, "en la normativa española se configura la acción de *habeas data* como el ejercicio de un derecho *personalísimo*"[104], advertimos que el reconocimiento de "los tradicionales derechos

[101] Enrique Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, (Madrid: Editorial Dykinson S.L, 2017), 267.
[102] Ávila Santamaría, *Los derechos y sus garantías. Ensayos críticos,* 264.
[103] Cfr. Guía legislativa de la OEA.
[104] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 152.

de la personalidad como derechos fundamentales ha supuesto un paso decisivo para precisar su *status* jurídico y su propia significación. Estos derechos, como se ha indicado, suponen la concreción y explicitación del valor de la dignidad humana"[105]. Así, la importancia del *habeas data* es esencial, por cuanto, dentro del Estado constitucional de derechos, la justiciabilidad de las libertades reconocidas en la Constitución exige "una plenitud constitucional que llena al detalle el ordenamiento jurídico, dejando menos ámbito para la Ley"[106].

De este modo, entendiendo a la dignidad "como la necesidad de que todas las personas sean consideradas y respetadas, y la proscripción de la instrumentalización del ser humano"[107], el derecho fundamental a la protección de datos plantea que "el tratamiento adecuado de los datos personales es una exigencia de la dignidad de la persona y del libre desarrollo de la personalidad"[108]. Por todo ello, es necesario precisar el significado de dignidad humana, para luego, considerar algunas apreciaciones respecto al derecho a la protección de datos personales.

En primer término, entendemos que la dignidad humana "exige el respeto por todos los derechos de todas las personas: nada es más prioritario que el derecho a vivir con dignidad"[109]. También J. Bidart Campos apunta que del concepto de dignidad humana "derivan los derechos personalísimos, como los derechos a la vida, a la integridad física y psíquica, al honor, a la privacidad, al nombre, a la propia imagen, al estado civil, y el propio derecho a la dignidad personal"[110]. En este orden de ideas, recordemos que "existe la percepción de que los tratamientos abusivos de datos personales menoscaban una parte importante de nuestra vida"[111]; por ello, el

[105] Pérez Luño, *Derechos humanos, Estado de Derecho y Constitución,* 331.
[106] Cfr. Resolución de la Corte Constitucional 344.
[107] Ávila Santamaría, *Los derechos y sus garantías. Ensayos críticos,* 264.
[108] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 32.
[109] Amnistía Internacional, Derechos Humanos para la Dignidad Humana, (Madrid: Editorial Amnistía Internacional, 2005), 15.
[110] Germán Bidart Campos, *Teoría general de los derechos humanos*, (México: Instituto de Investigaciones Jurídicas, 1993), 79.
[111] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 33.

derecho a la protección de datos personales emerge del respeto a la dignidad como base fundamental para la protección de la información de carácter personal, frente a los abusos que pueden ejercerse dentro de su tratamiento, por parte del poder público y/o privado. En consecuencia, “no es lo verdaderamente significativo la naturaleza íntima o no de los datos que se conocen o tratan, sino que sea susceptible de afectar a la libertad y la dignidad del individuo; se pretende evitar la intromisión”[112].

Lógicamente, dicha protección también corresponde a las injerencias que puedan resultar de las arbitrariedades, que nacen del uso indebido de las tecnologías de la información y comunicación. Con referencia a este aspecto, indicamos que “existe el peligro de que las tecnologías de la información entren en conflicto con el derecho a la intimidad y con el resto de los derechos fundamentales. La informática facilita ilimitadas posibilidades para recoger datos personales, tratarlos, conservarlos y transmitirlos”[113]. En todo caso, “el desarrollo de fenómenos como el Big Data, el Internet de las cosas, la decisión algorítmica, el aprendizaje automático o la inteligencia artificial ponen en jaque elementos fundantes del sistema de protección de datos, tal como la noción de consentimiento”[114].

> Es por ello, por los nuevos peligros y amenazas que el tratamiento informático trae consigo, por lo que se sugiere una conceptuación del derecho a la autodeterminación informativa que extienda su protección al uso ilícito o abusivo de la informática, frente a cualquier información en "manos de terceros" que represente una amenaza para la persona; la interceptación no consentida de la información, debe controlarse y limitarse sin detenerse a averiguar la índole íntima o no de la información[115].

En virtud de la diversidad de bienes jurídicos que pueda afectarse, mediante el abuso y uso indebido de la información de carácter personal, el replanteamiento del derecho a la protección de datos se precisa más que necesario. En una sociedad en donde el desarrollo de las tecnologías se ha convertido en una prioridad, la protección integral de la persona merece especial atención, debido a los riesgos

[112] Herrán, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, 53.
[113] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 46.
[114] Milanes, “Desafíos en el debate de la protección de datos para Latinoamérica”, 19.
[115] Herrán, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, 54.

que representan las Tics en el ejercicio de las libertades personalísimas. Desde esta perspectiva, el derecho a la protección de datos personales supone que la persona sea tratada conforme a su ser. Implica una condición que limita el ejercicio del poder público y privado, a partir del respeto a la igualdad de todas las personas. En suma, solidariamente, pretende concretar en beneficio de los ciudadanos –no desde la esfera individual, como un ente aislado, sino como un ser social que vive en comunidad– seguridad jurídica, frente al desarrollo de las tecnologías de la información y comunicación.

Finalmente, queda por señalar que la Constitución ecuatoriana precisa la protección de los derechos sobre la base de la dignidad humana[116]. Por tanto, dentro del modelo neoconstitucional ecuatoriano, tiene pleno sentido asumir que el derecho a la protección de datos emerge desde el valor más alto que representa la protección de los derechos fundamentales, la dignidad humana.

## 6.1 Definición del contenido del derecho fundamental a la protección de datos personales

Los progresivos cambios, en el marco regulador de la información personal, han instituido en la configuración de este derecho varias denominaciones que pretenden abarcar, no solamente su fundamento sino también el carácter autónomo del bien jurídico que se protege, frente al tratamiento de la información. Una de las principales fuentes de este cambio constituye los avances tecnológicos, que exigen del Derecho la articulación de nuevos principios.

Puede decirse que “la modernidad no sólo ha significado el más radical y antes insoñado salto tecnológico y científico de género humano, sino la consolidación de valores nuevos, y el derrumbe de otros”[117]. Hasta ahora, la priorización sobre el acceso a las tecnologías sigue siendo una de las principales características de la

[116] El Preámbulo de la Constitución de la República del Ecuador refiere la fundamentación del Estado Constitucional de Derechos sobre: “una sociedad que respeta, en todas sus dimensiones, la dignidad de las personas y las colectividades”.
[117] Nikken, “Sobre el concepto de Derechos Humanos”, 46.

sociedad moderna. No obstante, existe una desvalorización de los riesgos que supone la sobreexposición de la persona y de su información personal. Por estas razones, particular importancia tiene la definición de los elementos que componen este derecho fundamental, frente a prácticas ilícitas que afectan a los bienes jurídicos que tutelan la libertad para la autodeterminación informativa.

Afirmado como un derecho fundamental, la protección de datos o derecho a la autodeterminación informativa tiene su máxima expresión en el respeto de la dignidad humana[118], por cuanto se considera como un instituto de garantía de otros derechos fundamentales. En este orden, su objeto es "la protección de los datos, pero como fin último, la tutela de un plexo de bienes jurídicos que son específicamente atacados por el tratamiento de datos, y que se pretende con su creación brindar una tutela especial a las personas"[119]. Por ello, hay que entender que, "cuando se menciona el concepto de dato, éste no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar sus derechos, sean o no fundamentales"[120]. En todo caso, este derecho:

> Persigue que la protección de la identidad del individuo (persona física) sea realmente efectiva en un momento en que la tecnología permite que la información viaje sin restricciones y cuya recopilación masiva pone en riesgo el libre desarrollo de la personalidad atacando los resortes de los derechos humanos que están basados en el respeto a la dignidad humana[121].

---

[118] Según Lucas Murillo de la Cueva, la expresión "derecho a la autodeterminación informativa" puede ser considerada como "más expresiva" –que otras adoptadas por los legisladores y la doctrina– para hacer referencia al derecho fundamental a la protección de datos de carácter personal. Cfr. Lucas Murillo de la Cueva y José Luis Piñar Mañas, El *derecho a la autodeterminación informativa*, 11. En todo caso, Serrano Pérez agrega que "la libertad informática y la autodeterminación informativa son términos más coincidentes aludiendo en ambos casos al nuevo derecho fundamental resultado de la incorporación de la informática a las sociedades contemporáneas". Cfr. María Mercedes Serrano Pérez, "El derecho fundamental a la protección de datos. Su contenido esencial", *Anuario multidisciplinar para la modernización de las Administraciones Públicas*, Nro. 1 (2005): p. 252.

[119] Oscar Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de *habeas data* a dos décadas de su creación", en Eduardo Ferrer y Arturo Zaldívar (coord.), *La Ciencia del Derecho Procesal Constitucional: Procesos Constitucionales de la Libertad*, (México, Instituto de Investigaciones Jurídicas, 2008), 792.

[120] De la Serna Bilbao, "Las tecnologías de la información; derecho a la privacidad, tratamiento de datos y tercera edad", 9.

[121] Eduardo López y Juan Mora, "Un análisis de la estructura institucional de protección de datos en España: Un análisis jurídico y económico de la incidencia de las autoridades de control españolasen

El desarrollo de las denominadas tecnologías de la información y comunicación también afecta al tratamiento de los datos personales, como resultado de su circulación ilimitada y el libre acceso que se puede ejercer en una sociedad en red. Así, hay que considerar que la tecnología "es capaz de mover un gran volumen de información y de ponerla en relación, de manera que se construyan perfiles de nuestra personalidad"[122], evidentemente, sin mediar el consentimiento de las personas. Por ello, Puccinelli nos recuerda que, frente a la aparición del poder informático, estamos ante un derecho con contenidos diferenciales, el cual se constituye por "la suma de principios, derechos y garantías establecidos en favor de las personas que pudieran verse perjudicadas por el tratamiento de los datos de carácter personal a ella referidos"[123].

Sobre la definición de datos de carácter personal, la doctrina, la jurisprudencia y la legislación, en el ámbito internacional, coinciden en precisar que constituye cualquier información concerniente a una persona que la identifique o la puede hacer identificable, y que en todo caso pueda "facilitar la configuración de un perfil, aunque no pertenezcan al reducto de la intimidad de la persona"[124]. Así, por ejemplo, encontramos "los datos sobre los gustos o aficiones de las personas e, incluso, aquellos que puedan parecer irrelevantes para incidir en la dignidad como el color de pelo o el número de pie que se calza"[125]. Igualmente, advertimos que las tecnologías aplicadas al tratamiento de datos personales "crean un escenario en el que es posible que terceros, públicos o privados, reúnan tal caudal de información sobre las personas, que, prácticamente, no queden aspectos de su vida al margen del conocimiento ajeno"[126].

---

la garantía del derecho fundamental de autodeterminación informativa", *Indret – Revista para el análisis del derecho*, Nro. 2 (2009): p. 7.

[122] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 46.

[123] Puccinelli, "Tipos y subtipos de *habeas data* en América Latina", 2.

[124] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 133.

[125] De la Serna Bilbao, "Las tecnologías de la información; derecho a la privacidad, tratamiento de datos y tercera edad", 9.

[126] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 15.

Formalmente, el concepto de autodeterminación informativa aparece en la Sentencia del Tribunal Constitucional alemán de 15 de diciembre de 1983[127]. A ésta se le atribuye, por ejemplo "el mérito de haber configurado el derecho a la intimidad como expresión de un derecho a la autodeterminación informativa"[128]. Así también, con referencia a la dignidad humana y desarrollo de la personalidad, se le atribuye, además, establecer "una garantía jurisdiccional de protección de datos personales, siendo esto una concreción del derecho a la autodeterminación informativa"[129]. Por tanto, tratándose "de una especificación del derecho fundamental a la intimidad, que deriva del valor de la dignidad humana, el derecho a la protección de datos personales forma parte de los llamados derechos de la personalidad, cuyo ejercicio es de carácter personalísimo"[130].

Ahora bien, en el derecho a la protección de datos personales, el *habeas data* concreta "derechos y deberes que operan en el marco objetivo ofrecido por los principios de calidad de los datos"[131]. Evidentemente, este derecho fundamental se encuentra, ineludiblemente, vinculado al *habeas data,* "entendido éste como "derecho" y no, como preferimos por resultar más propio y fiel a su concepción originaria, como acción procesal constitucional"[132]. Por ello, tampoco resultaría equívoco mencionar que el *habeas data* nace también a partir del desarrollo tecnológico y, en suma, del avance de las tecnologías de la información y comunicación en una sociedad digitalizada. Entre los objetivos de esta garantía se encuentran que el accionante conozca qué tecnologías se usan para almacenar la información y también qué seguridades ofrecen los responsables del tratamiento de la información, con el fin de precautelar que los datos personales no sean utilizados, ilícitamente, en las instituciones públicas y privadas.

---

[127] Cfr. Gregorio, "Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina", 310.
[128] Aristeo García González, La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado, *Boletín Mexicano de Derecho Comparado*, Nro. 120 (2007): pp. 743-778.
[129] Ibíd.
[130] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 152.
[131] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 18.
[132] Puccinelli, "Tipos y subtipos de *habeas data* en América Latina", 1.

Por tanto, consideramos que el *habeas data* se presenta como un mecanismo de protección y tutela de la información de carácter personal, frente al tratamiento automatizado, derivado de entornos vinculados con las tecnologías de la información y comunicación. En este punto, asumimos que *el habeas data* refiere:

> Al amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad[133].

Desde esta perspectiva, la protección de datos supone una tutela más amplia que la que, tradicionalmente, ofrecía el derecho a la intimidad. Gran aporte sobre esta conceptualización también la desarrolló el Tribunal Constitucional de España[134], el cual en la Sentencia 292/2000 –a más de individualizar este derecho fundamental, del derecho a la intimidad– alude al extenso marco que comprende su protección, mediante la llamada libertad informática[135]. Así, este Tribunal afirmó que el derecho a la protección de datos "persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado". Por tanto, "no es ya

[133] Miguel Davara, *Anuario de Derecho de las Tecnologías de la Información y las Telecomunicaciones (TIC) 2002. Trabajos doctrinales especializados, boletines de actualidad, reseñas de interés jurídico, glosario de términos, preguntas más frecuentes y otras informaciones de interés*, (Madrid: Fundación Airtel, 2005), p. 3.

[134] La STC 292/200 del Tribunal Constitucional considera que: "La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad". Evidentemente, "la meritoria —por expresa y vanguardista— referencia a la informática en el texto constitucional de 1978 constituyó un innegable aldabonazo para otorgar trascendencia constitucional a la necesaria protección del individuo frente a los riesgos que sobre él —y, particularmente, sobre el disfrute de algunos de sus derechos fundamentales— cernían los avances tecnológicos ligados a la incipiente y primaria computerización". Cfr. Rallo Lombarte, "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)", 642.

[135] Así también la STC 292/200 advierte que el derecho reconocido en el art. 18.4 de la C. E. contiene "un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos que, además, es en sí mismo «un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática», lo que se ha dado en llamar «libertad informática»".

una libertad física, sino moral, que evita que se condicione la actuación de la persona a través de la información que otros tengan sobre ella"[136].

En este aspecto, agregamos que:

> La unión entre las tecnologías informáticas y las libertades constitucionales ha generado el nuevo derecho de libertad informática (…) Por tanto, hay que considerar la libertad informática como una libertad constitucional, que puede deducirse constitucionalmente, bien derivándola y haciéndola emerger de los principios constitucionales a través del trámite efectuado los tribunales constitucionales, o bien puede ser constitucionalizada, y en consecuencia, reconocida y determinada en el articulado de la Constitución, como así ha ocurrido en numerosas cartas constitucionales aprobadas recientemente en Europa y en el continente latinoamericano[137].

Así, como una garantía de libertad que se deduce de la normativa constitucional "se habla de un *habeas data* como un conjunto de instrumentos procesales –acceso, rectificación y cancelación– que garantiza que la persona dispone de un control sobre sus datos personales y, por tanto, una protección sobre su identidad personal"[138]. Por consiguiente, existen dos aspectos de singular importancia en materia de tratamiento de la información de carácter personal. El primero se refiere al control de los datos personales; y el segundo relacionado con el deber de respetar, en sociedad, el derecho a la protección de dichos datos.

En este contexto, advertimos que el tratamiento de la información debe ajustarse a ciertos principios, encaminados a proteger los derechos personalísimos que se derivan del derecho a la protección de datos personales. La importancia en este ámbito implica también determinar hasta qué punto se posee la facultad de compartir y utilizar la información. Por tanto, considerando que la tipología de datos personales es diversa, precisamos la necesidad de establecer límites y control, frente al tratamiento de la información, con el objeto de garantizar su efectivo cumplimiento. En este sentido, especial referencia debe hacerse a la categoría de datos personales que se consideran como sensibles o, especialmente protegidos.

---

[136] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 51, 52.
[137] Frosini, "Nuevas tecnologías y constitucionalismo", 38.
[138] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 52.

### 6.2 Los datos sensibles o especialmente protegidos

Inicialmente, los debates legislativos estuvieron enmarcados en concentrar la protección de datos personales, en los derechos de intimidad y privacidad de las personas. Por tanto, primeramente, surge la necesidad de distinguir el concepto de intimidad y privacidad, a fin de contextualizar el sentido de los datos sensibles, en el marco del derecho a la autodeterminación informativa.

Al respecto, exponemos que:

> Se ha afirmado que la intimidad es aquel ámbito de la vida de la persona que se sitúa por completo en la interioridad, fuera del alcance de nadie y, por tanto, ajeno a toda exteriorización y relación, mientras que la vida privada es aquella que se desenvuelve a la vista de pocos, o de otra persona y, en una aceptación más amplia, el conjunto de actos que se realizan o piensan para conocimiento de las personas cercanas[139].

De esta forma, la intimidad comprende aquel ámbito de la persona que se encuentra alejado de toda posibilidad, de conocimiento de terceras personas, es decir, está en lo más interno del ser y fuera del alcance de cualquier persona. Mientras que, la privacidad sería susceptible de ser revelada a determinadas personas. Ahora bien, distinguimos una tipología de datos que corresponden a la esfera de la intimidad, los cuales suponen una protección especial. Se hace referencia, en este sentido, a los datos sensibles o especialmente protegidos. Esta tipología de datos pertenece al ámbito íntimo de la persona. “Es una información que se reserva para uno mismo o para los más cercanos y su conocimiento afecta gravemente a la intimidad personal y familiar y al libre desarrollo de la personalidad, teniendo un enorme potencial discriminador”[140]. Por ello, “cuentan con una protección especial singularmente reforzada dado que forman parte de la esfera más íntima de las personas”[141].

---

[139] Pedro Serna, “Derechos fundamentales: el mito de los conflictos. Reflexiones teóricas a partir de un supuesto jurisprudencial sobre intimidad e información”, *Humana Iura: suplemento de derechos humanos,* Nro. 4 (1994), 197-234.

[140] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 782.

[141] De la Serna Bilbao, “Las tecnologías de la información; derecho a la privacidad, tratamiento de datos y tercera edad”, 15.

En este marco, es esencial determinar qué datos pueden considerarse como sensibles, frente al tratamiento de la información personal. Por ejemplo, dentro de esta categoría se encuentran "los datos personales que revelan origen racial y étnico, opiniones públicas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual"[142]. Por tanto, bajo la condición de ocasionar un daño más grave a la dignidad humana y al libre desarrollo de la personalidad, advertimos que estos datos "se convierten en extremadamente sensibles mediante un sencillo cambio del fin que se persiguiera al momento de su recolección"[143]. Instrumentos internacionales como el RGPD y los Estándares de protección de datos personales para los Estados Iberoamericanos, introducen como principal novedad a los datos genéticos y biométricos, dentro de las categorías de datos sensibles o especialmente protegidos. Así, el RGPD –en las categorías especiales de datos personales– manifiesta la prohibición del tratamiento de "datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física" –art. 9.1–. En el mismo sentido, los Estándares consideran que los datos personales sensibles incluyen "datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física" –art. 2.1. b)–.

Esta distinción, entre las categorías generales y las sensibles o especialmente protegidas de datos personales, responde:

> Lógicamente, a que los tratamientos de datos personales de opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, origen étnico o racial, salud, genéticos, biométricos dirigidos a identificar de manera unívoca a una persona física o relativos a la vida sexual o a las orientaciones sexuales suponen una grave injerencia en el derecho a la protección de datos personales y en otros derechos fundamentales como la libertad religiosa, la libertad ideológica, la libertad sindical o el derecho a la intimidad, de los que la protección de datos personales es también una garantía institucional[144].

[142] Víctor Bazán, "El *habeas data* y el derecho a la autodeterminación informativa en perspectiva de Derecho Comparado", *Estudios Constitucionales: Revista del Centro de Estudios Constitucionales*, Nro. 2 (2005), 85-139.
[143] Ibíd., 116.
[144] Antonio Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada*, Nro. 49 (2018), 187-266.

Puede decirse que los datos personales se clasifican tomando en cuenta su mayor o menor relación con el concepto de dignidad y ejercicio de los derechos fundamentales. Bajo el concepto de datos sensibles o especialmente protegidos, existen ciertos datos que no pueden ser objeto de injerencia u otras intromisiones, por comprometer un alto grado de afectación a la dignidad, intimidad personal y familiar y al libre desarrollo de la personalidad[145]. Por tanto, corresponde destacar que "los datos relativos a la ideología, religión, afiliación sindical o creencias, salud, origen racial o vida sexual cuentan con un tratamiento especial, de tal forma que nadie está obligado a facilitar dichos datos, salvo que una Ley habilite al efecto"[146].

En la actual sociedad globalizada, aparentemente, la dimensión que comprende la tutela del derecho a la protección de datos personales no se encuentra, debidamente, asociada como un derecho fundamental. Recordemos que la protección de esta libertad "no nació como un derecho —y en muchas latitudes sigue negándosele tal naturaleza—, pero resulta relevante resaltar su consolidación actual como tal —incluso caracterizándolo como derecho fundamental— tras protagonizar una historia de éxito al amparo de bases jurídicas que lo han forjado en el ámbito supranacional"[147]. Desde la inobservancia de los principios que engloban la tutela de los datos personales, hasta el uso ilícito de la información personal nos permite entender que aún queda mucho por hacer en la práctica. De hecho, en el ámbito público, un dato o determinada información puede tener un grado de interés general; sin embargo, debemos tener presente que este derecho fundamental protege también los datos que son de conocimiento público, por cuanto constituye la información que pertenece a una persona.

Por tanto, distinguimos "un conjunto de datos que se encontrarían en una zona de *core* y que tienen una muy elevada capacidad para impedir las injerencias"[148]. En

[145] Cfr. Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 781, 782.
[146] De la Serna Bilbao, "Las tecnologías de la información; derecho a la privacidad, tratamiento de datos y tercera edad", 16.
[147] Artemi Rallo Lombarte, "El nuevo derecho a la protección de datos", *Revista Española de Derecho Constitucional*, Nro. 116 (2019), 45-74.
[148] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 781.

esta zona, se encontrarían los datos especialmente protegidos y que, consecuentemente, pertenecen a la vida íntima del titular de la información. “Se trata de tratamientos sobre los que una sociedad debe estar alerta porque son sospechosos de ser discriminatorios”[149]. Anteriormente, señalamos que el derecho a la protección de datos personales se tutela, a través, del *habeas data*. Así, considerando que esta garantía faculta al titular de la información personal conocer y controlar el tratamiento y finalidades sobre el uso de su información personal, a continuación, abordaremos estos aspectos.

### 6.3 El control de la información personal y ejercicio de los derechos

El derecho a la protección de datos personales se fundamenta en “garantizar a los ciudadanos unas facultades de información, acceso y control de los datos que le conciernen (…) en el seno de sus relaciones con los demás ciudadanos y con el poder público”[150]. De hecho, “la otra parte del contenido esencial del derecho a la protección de datos la constituye un conjunto de derechos que garantizan la protección de la persona, frente al manejo de datos personales, es decir, garantizan la eficacia del consentimiento y del control”[151].

Uno de los principales problemas que enfrenta la protección de datos –junto a la imprecisión de conceptos debido a la complejidad del lenguaje que utiliza el legislador– es el desconocimiento de su contenido esencial, por tratarse de un derecho nuevo, al menos en el contexto latinoamericano. En este caso, advertimos que:

> El desconocimiento no es algo exclusivo de los ciudadanos. Se extiende a instituciones públicas y privadas que disponen de amplios volúmenes de información personal y, a veces,

[149] Troncoso, “Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales”, 227.
[150] Antonio Pérez Luño, *Manual de Informática y Derecho, (*Madrid: Editorial Ariel S.A, 1996), 44.
[151] María Mercedes Serrano Pérez, “El derecho fundamental a la protección de datos. Su contenido esencial”, *Anuario multidisciplinar para la modernización de las Administraciones Públicas*, Nro. 1 (2005): 253.

> va acompañado por un escaso celo, cuando no despreocupación, en la aplicación de las normas legales y reglamentarias que la protegen[152].

Así, la protección de datos implica, no solo, la voluntad individual, sino el quehacer de toda la sociedad[153]. Frente a este supuesto:

> Figuras como la de los principios de minimización y responsabilidad proactiva o el derecho a la portabilidad, como así también el mayor detalle y análisis de viabilidad de medidas concretas en cabeza de los responsables que aseguren el mejor tratamiento posible de los datos personales se presentan como de discusión necesaria[154].

Desde el titular de los datos personales, hasta quienes ejercen la responsabilidad de tratar información, tienen bajo su responsabilidad el cumplimiento de una serie de principios, deberes y facultades que merecen una necesaria aclaración con el objeto de garantizar, integralmente, el respeto de este derecho fundamental, a partir del concepto de la dignidad humana. Es imprescindible, entonces, centrar el debate en la preocupación sobre el desconocimiento del contenido de este derecho y las facultades que se atribuyen a los titulares de la información personal, frente al tratamiento ilícito. Si bien "la protección de datos personales debe acompasarse atendiendo a la mayor o menor cercanía con otros derechos fundamentales"[155]. Es, esencialmente, importante conceptualizar las facultades que comporta el control de la información personal. El tratamiento de la información personal debe respetar los elementos que componen este derecho fundamental, con el objeto de equilibrar la regulación y/o susceptibilidad o no del tratamiento por terceros. En este plano, nos referimos a los principios que deben considerarse en el tratamiento de la información. Por ejemplo, la confianza, seguridad, intimidad, privacidad y confidencialidad, como elementos esenciales en el tratamiento de la información;

---

[152] Lucas Murillo de la Cueva, "La protección de los datos de carácter personal en el horizonte de 2010", 134.

[153] Recordemos que "la célebre fórmula kantiana de que nadie debe ser un medio para que otros cumplan sus fines, salvo que sea medio y fin al mismo tiempo, ha provocado que, a nivel jurídico, como describe Alexy, el artículo uno de la Ley Fundamental alemana, que proclama que el Estado tiene como fin realizar la dignidad, tenga más de 94 volúmenes de sentencias del Tribunal Constitucional Federal". Cfr. Ávila Santamaría, *Los derechos y sus garantías. Ensayos críticos,* 264.

[154] Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", 28.

[155] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 781.

constituyen principios que se tutelan, a partir de las garantías que ofrece el derecho a la protección de datos.

Al respecto, apuntamos que:

> Tomando como referencia el nuevo Reglamento europeo, es importante destacar que incorpora una serie de novedades regulatorias, como el registro de las actividades de tratamiento que debe llevar cada responsable, la privacidad por defecto y por diseño, la notificación en caso de violaciones de seguridad al interesado y/o a la autoridad de aplicación, la figura del delegado de protección de datos, la evaluación de impacto o riesgo[156].

Puesto que el *habeas data* atribuye a la protección de datos o derecho a la autodeterminación informativa un carácter instrumental, es inexcusable abordar las facultades de control y deberes de limitación, respecto al tratamiento de la información personal, por cuanto constituyen garantías que, desde la normativa constitucional, permiten controlar y limitar el tratamiento de datos personales. "Todo ello constituye el perfil y el fundamento del derecho y, por quedar elevado a la categoría de contenido esencial, se convierte en el límite de los límites para el legislador, de forma que cualquier regulación del mismo habrá que respetar su contenido esencial para no vulnerar la intención constitucional"[157]. No interesa en esta parte realizar un estudio conceptual acerca de la naturaleza del *habeas data*, como de hecho se apuntará más adelante, pero sí es necesario determinar su relación con las facultades de control sobre el tratamiento de la información.

En este contexto, indicamos que:

> Según las particularidades léxico-jurídicas del país de que se trate, puede conceptuarse al *habeas data* como una acción, una garantía constitucional, un procedimiento jurisdiccional de trámite especial y sumarísimo, un proceso constitucional o un recurso protectorio del derecho de autodeterminación informativa o derecho a la protección de los datos personales frente a posibles excesos del poder de registración, precisamente, de la información de carácter personal[158].

Cuando hacemos referencia a que el *habeas data* constituye un recurso protectorio, frente a los excesos del poder de registración, esta garantía para la protección de datos concreta un conjunto de facultades que están destinadas a tutelar el

[156] Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", 25.
[157] Serrano Pérez, "El derecho fundamental a la protección de datos. Su contenido esencial", 254.
[158] Bazán, "El *habeas data* y el derecho a la autodeterminación informativa en perspectiva de Derecho Comparado", 90.

tratamiento de la información personal y, en suma, garantizar el ejercicio, control y poder de disposición de los datos. Por ello, advertimos que:

> El control del titular de los datos personales no es abstracto, sino concreto, con una capacidad real de informarse, exigir el consentimiento, acceder, rectificar, cancelar y oponerse al tratamiento de sus datos de carácter personal. Este derecho fundamental equivale a conocimiento y control. Este control se desarrolla en dos momentos: el primero, en la decisión de entregar los datos personales; el segundo, durante todo el tratamiento de los mismos a través de los derechos de acceso, oposición, rectificación y cancelación, que permiten seguir la vida del dato personal[159].

De esta manera, conceptualizamos esta garantía con relación a lo que el fenómeno tecnológico representa, dentro del tratamiento de la información personal, puesto que "en Indoiberoamérica se refiere casi unívocamente a la acción procesal constitucional (…) Y decimos casi unívocamente, pues parte de la doctrina y jurisprudencia españolas y particularmente la Corte Constitucional de Colombia y la doctrina colombiana en general, llaman de este modo no a la acción ni al proceso, sino al derecho autónomo y fundamental"[160].

### 6.4 El *habeas data* como garantía para la protección de datos personales

Las garantías constitucionales consisten en mecanismos de tutela que disponen los ciudadanos para asegurar el cumplimiento de los distintos derechos fundamentales que se consagran en la Constitución, como norma suprema del Estado. Así, las garantías constitucionales constituyen "aquellos procedimientos que se utilizan para restaurar el orden constitucional desconocido o violado"[161].

Apreciamos que el problema de los derechos fundamentales no está en determinar su justificación, ni el reconocimiento interno de que los Estados deben formalizar en sus ordenamientos jurídicos. El principal dilema al que se enfrentan los derechos es la tutela y su ejercicio en la práctica. Por ello, las garantías constitucionales

[159] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 138.
[160] Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de *habeas data* a dos décadas de su creación", 795, 796.
[161] Raymundo Gil Rendón, *Derechos procesal constitucional,* (México: Fundap, 2004), 23.

constituyen mecanismos de tutela que, frente a la vulneración de derechos, tienen por objeto "restituir el estado de cosas anteriores a la violación, y además implica que se desarrollen plenamente los mandatos constitucionales, para ajustar la Constitución a la realidad y para influir y cambiar la realidad"[162].

La protección de los derechos fundamentales enfrenta nuevas realidades y desafíos. "La contundencia del derecho a la autodeterminación informativa, en tanto garantiza al individuo el control de sus datos, genera innumerables y permanentes situaciones de conflicto con otros derechos, también esenciales para su adecuado desarrollo"[163]. Por tanto, si se hace referencia a la protección de la información personal, el principal desafío es su tutela efectiva, frente al desarrollo de las nuevas tecnologías. En este aspecto, señalamos que:

> Las NT y las TIC permiten, en efecto, un reforzamiento de determinadas garantías jurídicas y una renovación de determinados procedimientos y acciones destinadas a tutelar a la ciudadanía de los Estados de Derecho. El *habeas data* (…) representaría una de esas nuevas modalidades de acción procesal destinada a reforzar el status jurídico de los ciudadanos en las sociedades tecnológicas[164].

Desde la teoría neoconstitucional –que plantea Estado constitucional de derechos y justicia– se exige que la garantía de los derechos corresponda a una tutela judicial efectiva, y que aseguren el bienestar colectivo, a través, del respeto de los derechos fundamentales reconocidos en la Constitución. Así, como advierte la CCE:

> Con el nuevo paradigma constitucional, la Constitución deja de ser un programa político y se convierte en norma jurídica (…) quien crea el derecho es el juez constitucional y quien establece el procedimiento de producción y unificación del ordenamiento jurídico es el control constitucional, siendo la propia Constitución considerada como una norma jurídica directamente aplicable, al tiempo que constituye fuente del resto del ordenamiento jurídico[165].

De este paradigma que plantea el Estado constitucional de derechos y justicia se desprende un significativo avance en el respeto y la garantía de los derechos fundamentales. La norma suprema, la regla de decisión es la Constitución y no la

---

[162] Ibíd.
[163] Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", 28.
[164] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 36-37.
[165] Cfr. Registro Oficial Suplemento 451 de 22 de octubre del 2008. Corte Constitucional del Ecuador. (2008). Resolución S/N.

Ley. El centro del Estado es el ser humano y, por tanto, como señala la CCE se crea "un Estado al servicio de las personas y garante de la efectiva vigencia de los derechos fundamentales inherentes a la persona"[166].

Asumiendo que el *habeas data* constituye un derecho y una garantía "que permite a toda persona conocer, actualizar y rectificar las informaciones que sobre ella hayan sido consignadas en bancos de datos y en archivos de entidades públicas o privadas, en defensa de sus derechos fundamentales"[167]; en el marco del Estado constitucional de derechos y justicia, las Administraciones Públicas y los particulares tienen el deber y la obligación de respetar este derecho reconocido, no solo en la normativa constitucional, sino en los instrumentos internacionales[168].En este sentido, "en el Estado de derechos se está reconociendo varios sistemas jurídicos. Entre otros, el sistema regional que proviene de la OEA o la Comunidad Andina, el sistema internacional que brota de los órganos del sistema de Naciones Unidas"[169].

Hasta aquí, hemos referido que el respeto de los derechos fundamentales no depende, únicamente, de su reconocimiento constitucional, sino que también exige del Estado garantizar las condiciones para su pleno reconocimiento y ejercicio. En este fin, la implementación de procedimientos constitucionales que tiendan a llevar a efecto los derechos, se presenta como un presupuesto de garantías mínimas en el deber del Estado, de respetar y hacer respetar las libertades consagradas en la Constitución. Naturalmente, en materia de protección de datos personales, hacemos referencia al *habeas data*.

---

[166] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-09-SEP-CC –CASO Nro. 14-09-EP– publicada en el Registro Oficial 18 de 03-sep.-2009.
[167] Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de *habeas data* a dos décadas de su creación", 796.
[168] En nuestro ámbito regional, un instrumento que se destaca es la Guía legislativa de la OEA. La Corte Interamericana de Derechos Humanos, a través, de la Opinión Consultiva OC-24/17 ha resaltado la importancia de su vinculación en el marco de regulación, respecto al derecho fundamental a la protección de datos y *habeas data*. Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-24/17 relativa a la identidad de género, e igualdad y no discriminación a parejas del mismo sexo, solicitada por la República de Costa Rica, 2017.
[169] Ávila Santamaría, *El Neoconstitucionalismo andino,* 57.

Respecto a las causas que, principalmente, promovieron el surgimiento de ésta garantía, consideramos que:

> La inquietud sobre las agresiones a la intimidad que podían desprenderse por usos indebidos de las NT y las TIC (…) suscitó un progresivo debate entre los teóricos del derecho, que luego influyó en algunas decisiones jurisprudenciales y se tradujo también en previsiones constitucionales y legislativas sobre la materia. La temática relativa al "*habeas data*" (…) pretendía establecer una garantía procesal frente a la vulneración de la privacidad realizada a través de usos indebidos o abusivos de equipos informáticos[170].

Si bien el *habeas data,* tradicionalmente, se asocia como una garantía que permite tener conocimiento y/o acceso sobre la información personal que obra en poder de terceros. En la actualidad esta garantía se orienta a proteger los derechos de los ciudadanos, frente al tratamiento ilícito de la información personal y que, esencialmente, "hace referencia al conjunto de los denominados derechos o facultades ARCO, es decir, a los derechos de Acceso, Rectificación, Cancelación y Oposición. Estas facultades conjuntamente constituyen el núcleo del derecho a la libertad informática o derecho de autodeterminación informativa"[171].

Lógicamente, las facultades que concede el *habeas data,* se encuentran, plenamente, identificadas con el ejercicio de los derechos ARCO. De tal suerte que, como señala Pérez-Luño Robledo, esta garantía se fundamenta en el "interés de las personas concernidas para tener acceso a los datos personales que les afecta. De ahí la posibilidad de ordenar el acceso a los registros o archivos de datos para constatar la autenticidad o corrección de lo expresado"[172].

Así también en palabras de Puccinelli:

> El *habeas data* o protección de datos personales, establece garantías mínimas de calidad y confiabilidad de los datos nominativos o personales que se recojan; el derecho de las personas a exigir que sus datos personales le sean exhibidos; el derecho a que sean rectificados y el derecho a excluir los datos privados mantenidos sin autorización[173].

---

[170] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 128.
[171] Ibíd., 115.
[172] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 114.
[173] Oscar Puccinelli, *El Habeas data en Indoiberoamérica*, (Santa Fe de Bogotá-Colombia: Editorial Temis S.A, 1999), 351.

En consecuencia, se convierte, actualmente, en la garantía de tutela del derecho a la protección de datos, frente al uso ilícito y disposición arbitraria, de la cual puede ser objeto la información personal dentro de una sociedad informatizada. Ahora bien, en virtud de los bienes jurídicos que se encuentran incardinados al *habeas data*, Gozaíni advierte que:

> Protege el derecho a la intimidad; pero al mismo tiempo se afirma que la defensa es de la privacidad, o de la dignidad humana, o el derecho a la información, o bien la tutela del honor, o de la propia imagen o perfil personal, o derecho a la identidad, o simplemente acotado a la autodeterminación informativa[174].

De esta manera, el *habeas data* se concibe como una garantía de protección constitucional de carácter instrumental, por cuanto si bien garantiza el ejercicio del derecho a la protección de datos, además tutela las libertades que se desprenden de este instituto de garantía. En todo caso, consideramos que, frente a las nuevas tecnologías, "el derecho de libertad informática asume una forma nueva del tradicional derecho de libertad personal, como derecho a controlar las informaciones sobre la propia persona, como derecho del *habeas data*"[175]. Precisamente, esta garantía permite que el titular de la información personal se pueda instruir "con qué garantías está almacenando esas informaciones y qué aplicaciones tecnológicas usa para conservar adecuadamente la información; es decir, qué seguridades ofrece el titular del archivo o base de datos para prevenir daños, manipulaciones o usos indebidos de los mismos"[176]. A esto, se añade que "la tarea de control de la existencia y funcionamiento de los bancos de datos, no solo debe quedar en manos del poder político, el cual a través de sus normas puede establecer la regulación más eficaz a cumplir por los titulares del poder informático; sino que debe recaer también en los particulares"[177].

---

[174] Osvaldo Gozaíni, *Derecho procesal constitucional: Habeas data-Protección de datos personales,* (Buenos Aires: Rubinzal-Culzoni Editores, 2001), 13.
[175] Frosini, "Nuevas tecnologías y constitucionalismo", 31.
[176] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 23.
[177] Luis Castillo Córdova, *Hábeas Corpus, Amparo y Habeas data,* (Lima-Perú: ARA Editores, 2003), 371. En todo caso, Frosini advierte que "la evolución jurisprudencial ha reconocido y afirmado este nuevo derecho de libertad en los términos de protección de la autonomía individual, como exigencia pasiva en relación con los detentadores del poder informático, con los particulares o con las autoridades públicas". Cfr. Frosini, "Nuevas tecnologías y constitucionalismo", 31.

Bajo estas consideraciones, el *habeas data* constituye un mecanismo de garantía que atribuye al titular de la información una protección, frente al impacto de las nuevas tecnologías de la información y comunicación, en lo que respecta al tratamiento de sus datos personales. Cardinalmente, se orienta a tutelar, no solamente el "acceso" sino también el "control" sobre la información de carácter personal. Es decir, se orienta a garantizar la protección de datos, frente al tratamiento "ilegítimo" y "no autorizado" de la información personal. Por ello, el *habeas data* se instituye como el procedimiento constitucional necesario para garantizar la actuación inmediata del órgano judicial correspondiente, en los casos de violación de derechos y libertades fundamentales que resulten afectados, como consecuencia del manejo de bancos de datos, tanto públicos como privados.

Con estos antecedentes, a continuación, se analizará el origen y desarrollo del derecho a la protección de datos personales y la garantía de *habeas data,* a partir del proceso de Reforma Constitucional de 2008, el cual supuso el advenimiento de la teoría neoconstitucional en el sistema jurídico ecuatoriano.

## 7. El derecho fundamental a la protección de datos personales en la Constitución ecuatoriana

### 7.1 Referencia al pensamiento bolivariano en el proceso constitucional de Latinoamérica

Uno de los proyectos políticos de mayor trascendencia en el marco latinoamericano ha sido el surgimiento del denominado "Socialismo del Siglo XXI"[178]. Esta corriente socio-política tiene su fundamento en la búsqueda y desarrollo de una sociedad más justa. Enmarca la posibilidad de una revolución en todos los niveles del Estado, según los distintos procesos democráticos y de participación ciudadana, en la toma de decisiones, desde los estamentos más segregados de la sociedad. Así,

[178] En Latinoamérica, como un antecedente al surgimiento de este modelo socio-político, el Socialismo del Siglo XXI hace referencia a los cuestionamientos que –a partir de 1992– en Venezuela se realizaron sobre el régimen partidista tradicional. El ascenso al poder de Hugo Chávez, en 1998, significó el inicio de la denominada "Revolución Bolivariana" que abriría el camino de un nuevo ciclo político, desembocando en el reconocimiento del "Socialismo del Siglo XXI".

teóricamente, Heinz Dieterich Steffa considera que el "Socialismo del Siglo XXI" y su nueva institucionalidad se compone de "la democracia participativa, la economía democráticamente planificada de equivalencias, el Estado no-clasista y, como consecuencia, el ciudadano racional-ético-estético"[179].

El "Socialismo del Siglo XXI", en Latinoamérica, constituye "un nuevo socialismo que podría sintetizarse en la siguiente fórmula: propiedad colectiva (no necesariamente estatal) de los medios de producción + democratización fundamental de todas las esferas de la vida social"[180]. Es decir, supone la sustitución de un Estado neoliberal, por un estado solidario y equitativo, basándose en una democracia participativa[181].

Concretamente, en el contexto ecuatoriano se considera que:

> El desarrollo del socialismo del siglo XXI y la Revolución Ciudadana en el Ecuador pasan por la conceptualización y dotación de contenido a la democracia ciudadana que, como decía antes, pasa por una redefinición del concepto de democracia. Pero también del concepto de participación organizada, de la participación del movimiento o partido de gobierno en el proceso y de las formas de empoderamiento de la sociedad civil[182].

Así como, en otros países de Latinoamérica, en Ecuador, este modelo surge como consecuencia del decaimiento de la política tradicional y que supone, a partir de la propuesta constituyente, la instauración de un sistema constitucional de derechos afianzado en la regulación, progresividad y protección de los derechos[183].

---

[179] Heinz Dieterich Steffa, "El Socialismo del Siglo XXI", Recuperado de: http://noblogs.org/oldgal/737/SocialismoXXI.pdf.

180 Atilio Borón, "El socialismo del siglo XXI: Notas para su discusión", en: *Los Nuevos Retos de América Latina: Socialismo y Sumak Kawsay* (Quito-Ecuador, SENPLADES, 2010), 112.

[181] Como apunta Juan Montaña Pinto, "entre los motivos estructurales del cambio constitucional vivido en el país en estos últimos años, se pueden citar, entre otros, el fracaso del modelo político oligárquico-empresarial y corporativo que dominó en el país en los últimos 25 años, la urgencia de reinstitucionalizar un Estado devastado por el tsunami del neoliberalismo criollo, o la necesidad de organizar la sociedad y el Estado sobre nuevos pilares éticos y estéticos relacionados con la vigencia efectiva y la materialización del discurso de los derechos humanos". Cfr. Juan Montaña Pinto, "Presentación", en Ramiro Ávila Santamaría, *Los derechos y sus garantías. Ensayos críticos,* 18.

[182] Ricardo Patiño, "Diferencias entre el socialismo del siglo XX y el socialismo del siglo XXI. La democracia participativa y el nuevo sujeto revolucionario"; en: *Los Nuevos Retos de América Latina: Socialismo y Sumak Kawsay* (Quito-Ecuador, SENPLADES, 2010), 133.

[183] En efecto, "aparte de las agendas feminista, ambientalista o neodesarrollista, una de las teorías jurídicas y de las agendas políticas más influyentes en el proceso constituyente de Montecristi fue

> En efecto, lejos de lo que podía pensarse a primera vista, el texto constitucional ecuatoriano vigente no es una sola Constitución, sino que el constituyente, como expresión del pluralismo social y político vivido dentro de la Asamblea de Montecristi, incorporó en el texto constitucional cuatro o cinco agendas constitucionales independientes y yuxtapuestas que conviven en un equilibrio precario, y que, dependiendo de las relaciones entre ellas, van a dar como resultado un modelo constitucional distinto[184]

Entre las cuatro o cinco agendas señaladas, conviene hacer referencia a tres de ellas para enmarcar de manera preliminar el concepto del "Socialismo del Siglo XXl". La primera que se vincula a la determinación de un modelo político que propuso la implantación de una visión antiimperialista y nacionalista del Estado. La segunda relacionada a la constitucionalización de derechos innovadores, dentro del texto constitucional. Y, la tercera sustentada en el pueblo como máxime del poder constituyente. Sobre esta base, el derecho fundamental a la protección de datos personales se reconoce, como tal, por primera vez en la Constitución de 2008.

Como veremos en los siguientes apartados, este derecho pertenece a estas dos últimas agendas que se relacionan con la constitucionalización de derechos innovadores[185], mediante la implantación de la denominada democracia participativa[186]. Para llevar a la práctica este modelo de agendas, el escenario propicio fue la denominada "Asamblea Constituyente" que surgió en Venezuela, a

---

justamente las aportaciones del neoconstitucionalismo, cuyos presupuestos influyeron en buena parte del texto constitucional, particularmente en la visión que ahora tenemos de los derechos y las garantías". Cfr. Juan Montaña Pinto, "Presentación", en Ramiro Ávila Santamaría, *Los derechos y sus garantías. Ensayos críticos,* 18.

[184] Luis Fernando Ávila, *Política, Justicia y Constitución*, (Quito-Ecuador: Corte Constitucional para el Período de Transición, 2012), 13, 14.

[185] Sobre la condición de que la protección de datos personales constituye un "derecho innovador", desde ya, en esta investigación, será importante asimilarla como tal, considerando que, tanto el ámbito público como el privado, se enfrenta al manejo de grandes cantidades de información de carácter personal y, por consiguiente, establece un conjunto de garantías que permiten enfrentar los excesos en el tratamiento de la información personal, producto de los cambios sociales, políticos, jurídicos y tecnológicos.

[186] Líneas arriba, habíamos mencionado que el neoconstitucionalismo andino nace de siete vertientes, entre ellas la democracia comunitaria. Hablar de democracia participativa, como un postulado del Socialismo del Siglo XXl, implica reconocer la existencia de una democracia comunitaria que, como señala Ávila Santamaría, "no deja de ser una manifestación de opinión que viene desde abajo, desde los mandantes"; y que, en relación al derecho a la protección de datos personales, veremos cómo se materializó mediante el fundamento del discurso legislativo que lo aprobó. Cfr., Ávila Santamaría, *El Neoconstitucionalismo andino*.

partir de la expedición de la Constitución Bolivariana de 1999; en Bolivia en 2005; y en Ecuador en 2007[187].

### 7.2 Del *habeas data* al derecho fundamental a la protección de datos personales en la Constitución de Ecuador

Por primera vez, en el texto constitucional de 1996, se incorpora el *habeas data* como una garantía de protección de la información personal contenida en bancos de datos e informes. Supuso la tutela del derecho a controlar y conocer el uso y finalidad de la información personal en las instituciones públicas o privadas[188]. Así, esta Constitución señalaba que:

> Toda persona tiene derecho a acceder a los documentos, banco de datos e informes que sobre si misma o sobre sus bienes consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su finalidad. Igualmente, podrá solicitar ante el funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquéllos si fueren erróneos o afectaren ilegítimamente sus derechos. Se exceptúan los documentos reservados por razones de seguridad nacional –art. 30–.

En 1997, la nueva codificación del texto constitucional no alteró la naturaleza del derecho que protegía la Constitución de 1996. El tenor de esta garantía constitucional fue, exactamente, el mismo. No obstante, la Constitución de 1998 advirtió ciertas variaciones en la fundamentación de la garantía del *habeas data*[189], señalando que:

> Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren

[187] La llegada al poder ejecutivo del ex presidente Rafael Correa Delgado, en 2007, supuso, entre otras propuestas de campaña electoral, una consulta popular nacional –de ideología bolivariana, bajo los preceptos del "Socialismo del Siglo XXI"– llevada a cabo el 15 de abril de 2007. Este proceso de consulta tenía como finalidad instaurar una Asamblea Constituyente de plenos poderes, que prepare el proyecto de Reforma Constitucional de la Carta Magna de 1998. Finalmente, aceptada por voluntad popular dicha convocatoria, la Asamblea inició la elaboración de la reforma en noviembre de 2007, para que, finalmente, en septiembre de 2008, el proyecto sea aprobado con el 64 por ciento de los votos válidos.

[188] La Constitución Política de 1996 entró en vigencia, a partir, de su publicación en el Registro Oficial 969 del 18 de junio de 1996.

[189] La Constitución Política de 1998 entró en vigencia, a partir, de su publicación en el Registro Oficial 1 del 11 de agosto de 1998.

> erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La Ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional –art. 94–.

De la lectura de ambos textos constitucionales –considerando que el *habeas data* aseguraba el ejercicio de los derechos de acceso, rectificación, cancelación y oposición–, planteamos necesario diferenciar el derecho de acceso en ámbito de la protección de datos, del derecho de acceso a la información pública, por cuanto suele confundirse el acceso a la información que obra en registros públicos, con el derecho de acceso a los datos de carácter personal.

Al respecto, señalamos que:

> No hay que desconocer, al objeto de evitar equívocos o confusiones, que la figura del acceso de los ciudadanos a los registros públicos posee una naturaleza jurídica manifiestamente distinta a la del *habeas data*. Este derecho de acceso a la información administrativa (…) responde a presupuestos diferentes del *habeas data*. En efecto, mientras que en este derecho se toma por objeto la información contenida en registros públicos, por tanto, se trata de información pública, en el *habeas data* el objeto de la acción de acceso se refiere siempre a informaciones o datos personales, es decir, privados[190].

En primer término, advertimos que "cuando el acceso a la información pública se ejercita sobre documentación donde exista un tratamiento de datos personales, el derecho de acceso entra en conflicto con el derecho a la protección de datos personales"[191]. Esto obliga a delimitar la naturaleza, tanto del derecho de acceso a la información pública como del derecho de acceso a los propios datos personales sometidos a tratamiento[192]. Naturalmente, en esta delimitación es clave diferenciar "los bienes jurídicos que se pretenden proteger, en especial cuando estamos frente

[190] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 118.

[191] Antonio Troncoso, "La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>", en Antonio Troncoso (Dir.), *Comentario a la Ley de transparencia, Acceso a la Información Pública y Buen Gobierno*, (Navarra, Aranzadi, 2017), 992.

[192] Es preciso señalar que, doctrinariamente, se distinguen diversos tipos y subtipos de *habeas data*, entre ellos, los propios e impropios. "Los primeros son aquellos reconocidos en estricta conexión con el tratamiento de datos de carácter personal, y los segundos, para resolver problemáticas conexas, pero bien diferenciables, como el acceso a la información el acceso a la información pública o el ejercicio del derecho de réplica". Cfr. Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de *habeas data* a dos décadas de su creación", 871, 872.

a regulaciones que admiten el ejercicio de otros derechos diferentes del derecho a la protección de datos personales (derecho de réplica, derecho de acceso a la información pública)"[193].

El desarrollo legislativo del derecho de acceso a la información pública plantea algunos conflictos, a la luz de la normativa de protección de datos personales. Por ello, es esencial la correcta precisión del ámbito de aplicación material de este derecho fundamental, toda vez que en el marco instrumental de su protección coexisten principios relacionados con la publicidad y confidencialidad de la información. En este contexto, "resulta necesario conciliar el respeto del derecho a la intimidad y a la protección de datos personales de los ciudadanos con el derecho del público a acceder a la información del sector público"[194].

Sobre esta cuestión, la CCE aclara que:

> El objeto del derecho a acceder a la información pública es diferente al protegido por la acción de *habeas data*, encaminada a la protección de los datos personales, por lo que la misma Constitución de la República previó la existencia de una garantía jurisdiccional particular, denominada precisamente "acción de acceso a la información pública". Tal es así, que los datos personales, en gran parte de los casos, están protegidos por la excepción de confidencialidad al principio de publicidad de la información[195].

La delimitación del ámbito de aplicación de estos derechos fundamentales es trascendental, a partir de la confusión que puede generar la garantía y respeto al acceso a la información pública, con relación a la protección de las libertades que se derivan del tratamiento de la información de carácter personal. Por una parte, precisamos que el derecho de acceso a la información "hace referencia a las facultades de información y control que corresponden a los poderes públicos para el cumplimiento de sus funciones. Incluir estas facultades administrativas tradicionales en la figura del *habeas data* puede conducir a graves equívocos y confusiones"[196]; y por otra, frente al derecho de acceso a los propios datos

[193] Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de *habeas data* a dos décadas de su creación", 883, 884.
[194] Lucas Murillo de la Cueva y Piñar Mañas, El *derecho a la autodeterminación informativa*, 164.
[195] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 0067-11-JD– publicada en el Registro Oficial Suplemento 281 de 03-jul.-2014.
[196] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 118.

personales sometidos a tratamiento, consideramos que la protección de datos pone, especialmente, de manifiesto la vigencia del principio de proporcionalidad, el cual significa un pilar esencial en la normativa de protección de datos. Por tanto, este principio "obliga a analizar la injerencia en el derecho fundamental a la protección de datos personales derivada del acceso a información pública a la luz del juicio de adecuación, de necesidad y de proporcionalidad en sentido estricto"[197].

Bajo estas consideraciones, el tratamiento de la información personal en entidades de naturaleza, tanto pública como privada, debe ordenarse conforme a los principios previstos para la garantía del derecho fundamental a la protección de datos personales[198]. Por ello, entendemos que la aplicación del principio de proporcionalidad supone analizar las injerencias en el derecho a la protección de datos, "derivado de los distintos niveles de publicidad, del plazo de cancelación, del número y la tipología de datos personales objeto de acceso o de publicidad y de los diferentes intereses públicos en presencia"[199]. En este sentido, es esencial llevar a cabo una ponderación y equilibrio entre el interés público en la divulgación de la información y los derechos de los afectados, especialmente, el derecho a la protección de datos[200]. "El reto en este ámbito, como hemos señalado

[197] Antonio Troncoso, "La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>", 1006.

[198] Como señala Pérez Luño: "En nuestra época se ha adquirido plena consciencia de que la información es poder y que ese poder se hace decisivo cuando, gracias a la informática, convierte informaciones parciales y dispersas en informaciones en masa y organizadas (…) La trascendencia económica de la información ha generado un apetito insaciable de obtenerla por cualquier medio y a cualquier precio y es directamente responsable de determinadas prácticas abusivas que hoy, por desgracia, acechan el libre ejercicio de la privacidad en nuestra vida cotidiana". Cfr. Pérez Luño, *Derechos Humanos, Estado de Derecho y Constitución*, 361-362.

[199] Antonio Troncoso, "La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>", 1007.

[200] Recalcando en la tesis de Pérez Luño debe señalarse que, en el marco del tratamiento de la información personal, se precisa un equilibrio entre el flujo de la información y la garantía de privacidad de las personas. De ahí que, "ese equilibrio precisa de un <<*Pacto social informático*>> por el que el ciudadano consiente en ceder al Estado datos personales, a cambio del compromiso estatal de que los mismos se utilizarán con las debidas garantías (…) En términos análogos, debiera resolverse el dilema que concierne a la informatización de datos realizada en el sector privado". Cfr. Pérez Luño, *Derechos Humanos, Estado de Derecho y Constitución*, 363.

reiteradamente, sigue siendo facilitar el acceso a la información respetando el principio de proporcionalidad"[201].

Ahora bien, a diferencia de los textos constitucionales de 1996 y 1997, la Constitución de 1998 cambia el precepto de "finalidad" de la información personal, por el de "propósito" que se tenga. Se incluye, además, la penalidad de solicitar indemnización por falta de atención, la cual ocasione algún perjuicio. También es importante señalar que para el caso de los documentos reservados relacionados con la defensa nacional se legitima el levantamiento del sigilo, a través, de procedimientos especiales, debidamente, establecidos en la Ley.

En todo caso, quizá, el aporte más significativo de la Constitución de 1998 no sea, únicamente, la indemnización por falta de atención, ni tampoco el levantamiento del sigilo de documentos reservados. Sin duda, un aporte significativo –que no se había considerado en los textos constitucionales, anteriormente, citados– fue el reconocimiento de la protección de los datos especialmente protegidos, por el cual se garantizaba:

> El derecho a guardar reserva sobre sus convicciones políticas y religiosas. Nadie podrá ser obligado a declarar sobre ellas. En ningún caso se podrá utilizar la información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica –art. 23.21–.

Hasta aquí, entendemos que la principal garantía para la protección de la información de carácter personal constituía el *habeas data*. Como apreciamos, la regulación del derecho a la protección de datos personales no fue un problema, propiamente, normativo, por cuanto su protección se consolidaba, desde el ámbito constitucional, por medio del *habeas data* y otros derechos como la intimidad personal y familiar. Desde luego, también en el caso de Ecuador, este reconocimiento "sólo puede ser considerado un antecedente embrionario de los que varias décadas más tarde –previo paso y escisión del derecho a la intimidad primero

[201] Antonio Troncoso, "La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>", 1025.

y del derecho a la autodeterminación informativa después– se conocerá como derecho a la protección de datos"[202].

La idea de contar con derechos nuevos que faciliten los procesos de integración evidenció que la protección de la información de carácter personal en América Latina debía formularse como un requisito sin condición. Así, el incremento del flujo transfronterizo de la información de carácter personal motivado "en la mayor integración económica y social resultante del funcionamiento del mercado interior, como así también el incremento dentro de la UE del intercambio de datos entre los operadores públicos y privados, incluyendo a las personas físicas, asociaciones y empresas"[203], influyeron en la promulgación de normas relativas a la protección de datos en el ámbito del comercio internacional.

En efecto, señalamos que:

> Probablemente sea un error pensar que hoy pensar que la protección de datos personales es solo una cuestión de derechos fundamentales. Para América Latina y otros países puede tener implicaciones comerciales, ya que no les resulta conveniente quedar fuera del área de transmisión segura de datos, incluyendo estos los del comercio electrónico[204].

En el caso de Ecuador, un ejemplo de este efecto fue la promulgación de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos. Si bien el punto de partida para la protección de datos personales en el constitucionalismo ecuatoriano fue en 1996, a través, del *habeas data*. Esta Ley sectorial introduce, por primera vez, la protección de la información personal, como una garantía normativa de tutela de las relaciones jurídicas que resulten del comercio electrónico y del uso de las telecomunicaciones[205]. En todo caso, además, evidenciamos que este derecho

[202] Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de *habeas data* a dos décadas de su creación", 786.
[203] Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", 20.
[204] Cfr. Gregorio, "Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina", 325.
[205] La Ley de Comercio Electrónico, Firmas y Mensajes de Datos entró en vigencia, a partir, de su publicación en el Registro Oficial Nro. 557 de la República del Ecuador, el 17 de abril de 2002. Respecto a la protección de datos personales, esta Ley señala que "Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por

fundamental surgió como resultado del advenimiento de la era informática. Así, "debido al vertiginoso desarrollo de la telemática se produjo –a la par de innumerables beneficios– un notorio agravamiento de la potencialidad dañosa de las operaciones de tratamiento (acceso, registración, elaboración, transmisión a terceros, etcétera) de datos de carácter personal"[206].

Como señala Aristeo García, frente al desarrollo tecnológico y la economía digital, el derecho fundamental a la protección de datos plantea:

> Una regulación tal como se ha venido haciendo en Europa, mientras que Latinoamérica ha tenido que recurrir en cierta medida a dicho modelo para implementar en cada uno de sus países una protección efectiva a los datos personales de sus ciudadanos. Por lo tanto, el ámbito latinoamericano han sido pocos los países quienes han logrado este objetivo. Más aún, son en menor medida aquellos quienes en su ámbito constitucional lo reconocen expresamente como un derecho fundamental"[207].

Según lo expuesto, se desprenden dos cuestiones trascendentales. La primera, el acercamiento del marco jurídico latinoamericano al europeo producto de la necesidad de integración comercial que exige niveles adecuados para el tratamiento y transferencias internacionales de datos personales; y la segunda relacionada con la protección de la información de carácter personal, a partir de un despliegue normativo que neutralice los efectos de las tecnologías en los derechos de las personas.

En el caso de Ecuador, hasta antes de 2008, el derecho a la protección de datos personales carecía de reconocimiento como un derecho fundamental, propiamente, dicho. No obstante, como ha quedado señalado, su protección estaba garantizada, por medio del *habeas data*. Finalmente, la Constitución de 2008 es la que –fundada

---

la Constitución Política de la República y esta Ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo" –art. 9–.

[206] Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de *habeas data* a dos décadas de su creación", 787.

[207] García González, La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado, 758.

sobre el principio de una sociedad que respeta, en todas sus dimensiones, la dignidad de las personas– reconoce, por primera vez, de manera específica el derecho a la protección de datos personales, como un derecho fundamental autónomo y de libertad[208].

### 7.3 La Reforma Constitucional de 2008 en Ecuador

La Asamblea Nacional Constituyente de plenos poderes elegida para la Reforma Constitucional de 2008 organizó su actividad de presentación y debate de propuesta de los textos constitucionales, bajo una metodología de consenso y participación plena de la sociedad en general[209]. A propósito del "Socialismo del Siglo XXI", el neoconstitucionalismo andino se idealizó, mediante un proyecto constitucional histórico afianzado en la garantía de los principios de los derechos fundamentales, los cuales permitieron avanzar en la interpretación del ejercicio y exigibilidad de los derechos más esenciales del ser humano, pre existentes en los instrumentos internacionales sobre derechos humanos[210]. Los debates legislativos de dicha

[208] La Constitución de la República del Ecuador de 2008, entró en vigencia a partir de su publicación en el Registro Oficial 449 de 20 de octubre 2008.

[209] Mediante elecciones libres, universales y directas celebradas el 30 de septiembre de 2007, el pueblo del Ecuador eligió a 130 representantes como sus mandatarios para conformar la Asamblea Constituyente, de los cuales 80 pertenecían al Bloque de Gobierno, denominado Alianza País, del Presidente Rafael Correa. El Poder Constituyente de la Asamblea afirmó que ésta asumía y ejercía "plenos poderes", es decir, según el Mandato Constituyente 1: "Las decisiones de la Asamblea Constituyente son jerárquicamente superiores a cualquier otra norma del orden jurídico y de obligatorio cumplimiento para todas las personas naturales, jurídicas y demás poderes públicos sin excepción alguna. Ninguna decisión de la Asamblea Constituyente será susceptible de control o impugnación por parte de alguno de los poderes constituidos. Asimismo, los jueces y tribunales que tramiten cualquier acción contraria a las decisiones de la Asamblea Constituyente serán destituidos de su cargo y sometidos al enjuiciamiento correspondiente. De igual manera, serán sancionados los funcionarios públicos que incurran o promuevan, por acción u omisión, el desacato o desconocimiento de las disposiciones de la Asamblea Constituyente".

[210] Según Ávila Santamaría, el proyecto político de la Revolución Ciudadana materializado en la Constitución de Montecristi en 2008, "tiene instituciones que no solamente abren la puerta a la imaginación de posibilidades de un mundo distinto, sino que constituyen una oportunidad para la transformación de la realidad". De esta manera, más personas son ciudadanos, mediante el reconocimiento de más derechos que los civiles y políticos. Cfr., Ávila Santamaría, *El Neoconstitucionalismo andino*.

Asamblea consagraron los principios de ejercicio y exigibilidad de los derechos, a través, del goce efectivo e inmediato de éstos y que, como señalan las actas legislativas que promovieron su constitucionalización, se enuncian en la Constitución, por medio, de la plena participación de la ciudadanía[211].

Con este antecedente, la Asamblea registró en el Acta Nro.50 el debate legislativo sobre el derecho a la protección de datos personales[212]. En una primera fase, la Mesa Constituyente Nro. 1 presenta para el primer debate el informe de mayoría y minoría de los textos constitucionales referente a los "derechos civiles, al debido proceso y una justicia sin dilaciones, políticos y a la comunicación"[213]. En lo que cabe a los derechos civiles –que incluyó a la protección de datos personales–, se presentó, en términos generales, la Carta de Derechos, en donde, entre otros aspectos, para su fundamentación se hacía referencia a estándares internacionales establecidos en diversos tratados de derechos humanos ratificados por Ecuador y que constituyeron las bases para el contenido mínimo de dicha Carta[214].

En este debate, se mencionó que se mantenía el contenido de los derechos civiles, políticos y de comunicación que fueron reconocidos en la Constitución de carácter neoliberal de 1998, con algunos avances, modificaciones e incorporaciones en lo

[211] En los antecedentes del acta 50 de la Asamblea Nacional Constituyente, en relación a la propuesta de Carta de Derechos, se considera que ésta surge, a partir, de un proceso amplio de reflexión colectiva con la ciudadanía: a) propuestas y sugerencias de más de 160 representantes de varios sectores de la población; b) 120 propuestas presentadas, mediante Internet; y c) 6 mesas itinerantes, con el objeto de recopilar propuestas y promover la participación ciudadana.

[212] El 15 de mayo de 2008 la Mesa Constituyente Nro. 1 de Derechos Fundamentales y Garantías Constitucionales, conformada por trece legisladores –ocho del bloque de gobierno (Alianza País) y 5 de oposición, escogidos de entre varios partidos políticos– ponen en conocimiento del Pleno de la Asamblea, para su primer debate, los textos constitucionales referentes a los derechos civiles, en donde se incluye el derecho a la protección de datos personales.

[213] Para el inicio de este primer debate sobre la Carta de Derechos Civiles –con ochenta y dos Asambleístas presentes en el seno legislativo–, según el informe del Asambleísta Jaime Abril, la propuesta fue aprobada por consenso con Informe de Mayoría, con excepción del Asambleísta Rafael Estévez, quien expuso su Informe de Minoría, pero que en nada hizo referencia a la aprobación del derecho a la protección de datos personales.

[214] Según el Acta 50 de la Asamblea, para la fundamentación de esta Carta de Derechos se realizó un proceso amplio de reflexión colectiva con la ciudadanía, recibiéndose más de 160 visitas de varios representantes de sectores de la población, quienes presentaron sus propuestas y sugerencias para incluir nuevos derechos o ampliar y ratificar los ya reconocidos en la Constitución de 1998; también vía Internet se recibieron 120 propuestas; además de la ejecución de 6 mesas itinerantes.

que al derecho a la protección de datos personales se refiere[215]. Desde esta perspectiva, el numeral 4 de la propuesta de derechos civiles señaló que "además se incluye y/o desarrollan algunos derechos como la objeción de conciencia; el derecho a la alimentación que incluye la dimensión de la seguridad y soberanía alimentaria; y a la protección de datos de carácter personal"[216].

Así, bajo el concepto de derecho a la protección de datos de carácter personal, se propuso el siguiente texto:

> Articulo innumerado. Derecho a la protección de datos de carácter personal: a) El Estado garantiza el derecho a decidir sobre los datos personales; b) La Ley regulará la recolección, archivo, procesamiento, distribución o difusión de la información de estos datos. Para todo esto se requerirá la autorización del titular o la prescripción de la Ley.

En este mismo bloque de propuesta legislativa sobre los derechos civiles, se hizo también especial referencia al derecho a la reserva de la información o datos sensibles de la siguiente manera:

> Articulo innumerado. Derecho a la reserva. Toda persona tiene derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades personales de atención médica.

Por otra parte, como un derecho fundamental, independiente de la protección de datos personales, aparecía en la propuesta el derecho a la intimidad. El texto se

[215] Según la Mesa Nro. 1, el carácter "neoliberal" de la Constitución de Ecuador de 1998 hacía alusión al carácter progresista en el reconocimiento de derechos. Así, en palabras de Ávila Santamaría el modelo neoliberal "intenta rescatar y renovar el ideal liberal decimonónico con algunos componentes que, al momento, no eran muy claros, como la democracia. El neoliberalismo, además, ha logrado incluir en el discurso conceptos de carácter emancipador, como los mismos derechos humanos, la participación, el acceso a la justicia y el género. Finalmente, el neoliberalismo, en lo internacional, propone una concepción de estado facilitador y menos rígido en cuanto a la soberanía decimonónica". Cfr. Ávila Santamaría, *Los derechos y sus garantías. Ensayos críticos,* 261. En todo caso, Ávila Santamaría advierte que "la Constitución de Montecristi recoge elementos que marcan el camino de lo que podría ser un constitucionalismo posliberal" y que, en suma, mantendrían la esencia de constituciones anteriores. Cfr., Ávila Santamaría, *El Neoconstitucionalismo andino*.

[216] Desde esta perspectiva –a diferencia de la Constitución de 1998, que incluía a los derechos civiles como numerales de un único artículo– la Mesa consideraba necesario que cada uno de los derechos a los que se hacía referencia en la Carta de Derechos Civiles deberían estar enunciados como artículos independientes para proporcionarles mayor énfasis y reconocimiento.

propuso de la siguiente manera: “Articulo Innumerado. Derecho a la intimidad personal y familiar”.

Sobre la Carta de Derechos Civiles, la Asambleísta María Molina [217] consideró que estos derechos definían la acción del Estado en función de la cual se debían organizar las estructuras del poder del Estado bajo un régimen innovador, revolucionario y progresista, el cual constituirá el inicio de un nuevo paradigma, en cuanto al goce y ejercicio de los derechos fundamentales[218]. Precisamente, al hacer referencia a un régimen de derechos fundamentales de carácter innovador y progresista[219], uno de estos precedentes invocaría el reconocimiento de la protección de datos personales, como un derecho autónomo. Con referencia a este aspecto, recordemos que el derecho a la protección de datos representa en el ámbito internacional un derecho innovador o una libertad informática caracterizada por la “evolución de la sociedad tecnológica, el derecho de libertad informática manifiesta un aspecto nuevo de la vieja idea de la libertad personal y constituye el avance de una frontera nueva de la libertad humana a través de la sociedad futura”[220].

En el inicio del debate legislativo sobre la Carta de Derechos Civiles, la primera referencia sobre el derecho a la protección de datos la realizó Leonardo Viteri. Este asambleísta propuso que en este artículo correspondería lo siguiente: “solo podrán

[217] Asambleísta de gobierno (Alianza País), ponente y presidenta de la Mesa Constituyente Nro. 1.

[218] Se considera en esta exposición que –a propósito de los sesenta años del nacimiento de la Declaración Universal de los Derechos Humanos, a la fecha en que la Asamblea Constituyente inicia el proceso de reforma constitucional– en última instancia estos derechos existen para proteger y asegurar el ejercicio y respeto de los derechos fundamentales en sus ciudadanos.

[219] Podemos tomar como referencia la alusión de que para la reforma constitucional de la Carta de Derechos Civiles propuesta por la Mesa Constituyente se amplía a treinta y cuatro derechos a diferencia de la Constitución de 1998 con veinte y seis derechos. Es importante destacar que la Ponente, Asambleísta María Molina, señala que la mayoría de los artículos propuestos, en esta parte por la Mesa Constituyente, fueron aprobados por unanimidad mientras que aquellos que no lograron alcanzar esta dimensión fueron consensuados por más del setenta y cinco por ciento de los asambleístas de la Mesa.

[220] Frosini, “Nuevas tecnologías y constitucionalismo”, 30. En todo caso, –debido al contexto tecnológico y los procesos de integración comercial, desarrollados una economía digital–, hay que considerar que “estamos ante un «nuevo derecho» de protección de datos, esto es, ante un nuevo marco normativo multinivel en el que interaccionan normas europeas y nacionales. Y tal vez no resultara exagerado interrogarse sobre si estamos ante un «nuevo derecho» de protección de datos”. Cfr. Rallo Lombarte, “El nuevo derecho a la protección de datos”, 48-49.

ser utilizados con fines estadísticos"[221]. Mención especial merecen las intervenciones de Jaime Abril[222] y Cristina Reyes[223], quienes destacan en la propuesta el análisis de los derechos de intimidad personal y familiar; y del derecho a la reserva, respectivamente. Sobre estos argumentos, corresponde advertir que la comprensión original de la propuesta, relativa al derecho fundamental a la protección de datos, era considerarlo como una libertad autónoma e independiente del derecho a la intimidad.

Como hemos destacado anteriormente, esta interpretación de los legisladores resultó equívoca a la hora de precisar la naturaleza y objeto del derecho a la protección de datos, por cuanto este derecho fundamental constituye una garantía sobre el tratamiento de la información personal, que requiere un necesario desarrollo en la normativa secundaria, no solo para la tutela de los datos personales sino, además, para la garantía de otros derechos y libertades fundamentales. Como se verá en los siguientes capítulos, sus principios, excepciones, derechos y obligaciones constituyen la base para articular en la práctica un marco jurídico equilibrado que garantice seguridad jurídica en el ámbito público y privado[224]. Por ello, si bien a criterio de los constituyentes debía agregarse en el texto constitucional cuestiones relativas al tratamiento de datos personales con fines estadísticos y, además, el respeto del derecho a la intimidad y a la reserva de la información; aclaramos que, siguiendo la experiencia internacional, estos presupuestos exigen

[221] Asambleísta del Partido Social Cristiano (PSC) considerado de centro derecha y de ideología neoconservadurista-humanista.
[222] Asambleísta de Gobierno e integrante de la Mesa 1.
[223] Asambleísta del Partido Social Cristiano (PSC).
[224] Como expone la CCE, "el Estado constitucional de derechos y justicia se refuerza cuando, además de promover la supremacía y aplicación directa de la Constitución de la República, se reconoce a la seguridad jurídica como derecho constitucional, el cual se fundamenta en el respeto a nuestro texto constitucional y en la existencia de normas jurídicas claras, previas y públicas por parte de las autoridades competentes". Véase el Registro Oficial Suplemento 607 de 14 de octubre del 2015 –Caso signado con el Nro. 788-14-EP–. Así también, sobre la importancia del derecho a la seguridad jurídica dentro del Estado constitucional de derechos, véase el Registro Oficial Edición Constitucional 34 de 14 de marzo del 2018 –Caso signado con el Nro. 1052-16-EP–; y Registro Oficial Suplemento 854 de 4 de octubre del 2016 –Caso signado con el Nro. 578-14-EP–.

desarrollarse sobre la base de una normativa de protección de datos clara y precisa que, en la práctica, garantice el derecho a la seguridad jurídica[225].

Así, para que el derecho a la protección de datos sea de aplicación "es necesario que se den los elementos que delimitan su objeto y su ámbito de aplicación: que exista un tratamiento y que éste se sustancie sobre datos personales"[226]. Del texto constitucional propuesto, se evidencia que "el Estado garantiza el derecho a decidir sobre los datos personales"; y así también que "la Ley regulará la recolección, archivo, procesamiento, distribución o difusión de la información de estos datos". Por tanto, en nuestro concepto estas definiciones son importantes al momento de conceptualizar este derecho fundamental, desde el ámbito constitucional.

Retomando las exposiciones relacionadas con el derecho a la protección de datos, Gissel Rosado[227] realizó observaciones al inciso que refiere "El Estado garantiza el derecho a decidir sobre los datos personales", bajo la perspectiva de que, sobre los datos personales, nadie puede decidir y que el Estado no puede inmiscuirse en ello. En este aspecto, si bien el derecho fundamental a la protección de datos es una garantía que "nace como un derecho a controlar la información personal frente a los tratamientos"[228], nos parece que el texto observado por el legislador fue equivocado, toda vez, que la facultad de controlar el tratamiento de la información personal recae

[225] Así, por ejemplo, respecto al tratamiento de datos personales con fines estadísticos, el RGPD precisa que: "el contenido estadístico, el control de accesos, las especificaciones para el tratamiento de datos personales con fines estadísticos y las medidas adecuadas para salvaguardar los derechos y las libertades de los interesados y garantizar la confidencialidad estadística deben ser establecidos, dentro de los límites del presente Reglamento, por el Derecho de la Unión o de los Estados miembros. Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos. Estos resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica. El fin estadístico, implica, que el resultado del tratamiento con fines estadísticos no sean datos personales, sino datos agregados, y que este resultado o los datos personales no se utilicen para respaldar medidas o decisiones relativas a personas físicas concretas" –Considerando 162–.

[226] Antonio Troncoso, "La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>", 976.

[227] Asambleísta del Partido Renovador Institucional Acción Nacional (PRIAN) considerado de centro derecha y de ideología populista.

[228] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 740.

también sobre los excesos o intromisiones del Estado o la Administración Pública. En todo caso, advertimos que la propuesta hacía referencia a la garantía de que el Estado debe incidir sobre el control y decisión de la información, frente a los tratamientos.

Ahora bien, Luis Hernández[229] propuso que se estime un derecho a la intimidad personal y de la familia bajo el siguiente texto: "Toda persona tiene derecho a la inviolabilidad de su vida familiar y privada, de su domicilio, de su correspondencia, así como de sus relaciones postales y de sus telecomunicaciones, toda persona tiene el derecho de ser protegido contra el empleo ofensivo de sus datos personales". Con referencia a este aspecto, apreciamos que el legislador confunde, nuevamente, la naturaleza del derecho a la protección de datos al situarlo como fundamento del derecho a la intimidad. Atendiendo a lo señalado, conviene insistir en que, tanto la doctrina como la jurisprudencia internacional, reconocen que" la protección de datos es un instituto de garantía de otros derechos fundamentales distintos del derecho a la intimidad"[230]; y que, en todo caso, comparte con éste el objetivo de "ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos"[231]

Así también el Asambleísta Lenin Hurtado[232] estimó que –cuando el texto propuesto refiere a la protección contra el tratamiento o el procesamiento– se debía agregar: "procesamiento, tratamiento automatizado, porque hay el peligro en los datos de carácter personal, que procesados automáticamente, puedan derivar en información que sea en contra de la misma persona titular de esos datos". Sobre

[229] Asambleísta del Partido Red Ética y Democracia (RED) considerado de izquierda y de ideología socialista.
[230] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 74.
[231] El Tribunal Constitucional de España agrega que, "la peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran". Véase la STC 292/200 del Tribunal Constitucional de España.
[232] Asambleísta del Partido Movimiento Popular Democrático (MPD) considerado de izquierda y de ideología socialista.

este punto, entendemos que el supuesto de tratamiento automatizado de la información es un fundamento que tiene plena validez, por cuanto es innegable la facilidad que las tecnologías pueden ofrecer, al momento de realizar intromisiones o injerencias en la vida privada de las personas. Por ello, advertimos que "se echa en falta un reconocimiento más claro tanto del derecho fundamental a la protección de datos personales, estén o no automatizados, como de la protección de los derechos frente a las nuevas tecnologías"[233].

Finalmente, el Asambleísta Sergio Chacón[234] estimó un exceso en la propuesta sobre el derecho a la protección de datos, manifestando que "el Estado garantiza el derecho a decidir sobre los datos personales". Por tanto, consideró que "el derecho a decidir sobre los datos personales, nos parece que puede ser contraproducente (…) debemos tener el derecho de acceder a nuestros datos, derecho a solicitar rectificaciones y a que se mantenga en reserva, en privacidad estrictamente las cosas que son privadas y personales, mas no los datos públicos".

Sobre esta última cuestión, precisamos que:

> Un acceso indiscriminado a información pública puede suponer una transparencia absoluta no sólo de la Administración, sino de los ciudadanos ante la sociedad, especialmente en el caso de los empleados públicos, lo que vulnera no sólo nuestro derecho fundamental a la protección de datos personales, sino también nuestro derecho a la intimidad, que es un presupuesto para una mínima calidad de vida, para la dignidad y para la libertad personal[235].

En el cierre de este primer debate, de los ochenta y dos Asambleístas presentes en la sesión legislativa señalada, a través, del Acta Nro. 50; cinco asambleístas hicieron referencia al derecho a la protección de datos personales, y dos analizaron en debate derechos relacionados con este instituto de garantía, es decir, sobre el derecho a la intimidad y derecho a la reserva de la información. En adelante, el debate no trascendió y, prácticamente, en nada se hizo referencia –incluido el segundo debate, sobre los derechos civiles– al derecho a la protección de datos.

---

[233] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 78.
[234] Asambleísta del Partido Sociedad Patriótica (SP) considerado centralista y de ideología populista.
[235] Antonio Troncoso, "La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>", 974.

Por otra parte, a pesar de que no existe una referencia específica en las actas legislativas, sobre el origen de la propuesta para considerar a la protección de datos como un derecho fundamental; interpretamos que la inserción de este nuevo derecho fue el resultado, tanto del proceso de reflexión colectiva con la ciudadanía, como así también de los estándares establecidos en instrumentos internacionales. En todo caso, en relación a la posición política del debate legislativo[236], si bien se evidencia que surge de partidos políticos, tanto de ideología de izquierda como de derecha. El origen de este derecho fundamental se estatuye, sobre la base, tanto de los principios del denominado Socialismo del Siglo XXl como de la teoría neoconstitucionalista, enmarcados, principalmente, en la denominada democracia participativa y en la constitucionalización de nuevos derechos fundamentales[237].

Bajo estas consideraciones, la Asamblea Nacional Constituyente registró, mediante el Acta Nro. 67 la votación de los textos constitucionales referentes a los derechos civiles, entre los que se encuentra el derecho a la protección de datos[238]. Siguiendo la formalidad del proceso legislativo, intervino la ponente de la Mesa 1, la Asambleísta María Molina[239], recalcando que a la luz de las observaciones presentadas en debate por los legisladores se analizaron y sistematizaron todos los derechos civiles, con la finalidad de acogerlos en un texto constitucional definitivo, según los criterios democráticos, de técnica jurídica y de pensamiento

[236] Véase Nota 120 y 123. Al respecto, hay que recalcar que la Mesa 1 de la Asamblea Nacional Constituyente estaba conformada por mayoría de legisladores de Alianza País –ocho de trece asambleístas– cuya tendencia política estaba orientada sobre la base de los principios del Socialismo del Siglo XXl. En todo caso, la Carta de Derechos Fundamentales y Garantías Constitucionales –que contenía el borrador del derecho fundamental a la protección de datos personales– fue aprobada por consenso en la Mesa y con informe de mayoría.

[237] Así, se advierte que, en la Constitución de 2008, "los derechos se han multiplicado en número y se han engrosado en contenido. El impacto de los derechos humanos en el derecho y en el Estado es enorme. Por un lado, la teoría del derecho se ha visto afectada por lo que se denomina ahora neo constitucionalismo; y el Estado ahora se legitima solo si cumple con los objetivos que constan en los principios determinados en la parte dogmática, que no son otros que los derechos humanos y que establecen límites constitucionales a todos los poderes". Cfr. Ávila Santamaría, *Los derechos y sus garantías. Ensayos críticos,* 185.

[238] El 24 de junio de 2008, la Mesa Constituyente Nro. 1 de Derechos Fundamentales y Garantías Constitucionales pone en conocimiento de la Asamblea, para aprobación, los textos constitucionales referentes a los derechos civiles, en donde se incluye el derecho a la protección de datos personales.

[239] La Asambleísta María Molina también formó parte de la Comisión de Redacción del articulado final de los derechos civiles, considerándolos a éstos como una de las conquistas más importantes de la humanidad, por lo que resguardan la esfera más íntima de la protección de la persona.

progresista[240]. De esta manera, la Secretaría de la Asamblea procedió a dar lectura de los textos constitucionales definitivos sobre los derechos civiles.

En relación al derecho a la reserva se señaló:

> Numeral 9.- Derecho a la reserva. - Toda Persona tiene derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación y/o pensamiento político; ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades personales de atención médica.

Sobre el derecho fundamental a la protección de datos personales:

> Numeral 18.- Derecho a la protección de datos de carácter personal. - a) Toda persona tiene derecho a acceder y decidir sobre información y datos de carácter personal y a que estos sean protegidos. b) Para la recolección, archivo, procesamiento, distribución o difusión de esos datos o información se requerirá la autorización del titular o la prescripción de la Ley.

Sobre la intimidad, "se reconocerá y garantizará: Numeral 19.- Derecho a la intimidad personal y familiar"[241].

Puede considerarse que, a partir, de la incorporación de la dignidad humana en los instrumentos internacionales en materia de derechos humanos, el reconocimiento de éstos han adquirido, subsidiariamente, valor jurídico, mediante su integración en los textos constitucionales de los Estados, como una de las bases del orden jurídico, político y social interno que los estados deben prever. En todo caso, como hemos destacado, dos de las instituciones que consolidan el Socialismo del Siglo XXl han sido la democracia participativa y la propuesta de derechos innovadores. Sobre la primera es indudable, antes y durante el proceso de la Asamblea Constituyente, la campaña que se ejerció por el neoconstitucionalismo andino. No obstante, la posibilidad de contar con derechos innovadores manifiesta la importancia de que el

[240] En este orden de ideas, los cambios principales realizados al texto definitivo, en relación a nuestro objeto de estudio, constituyen, por ejemplo, sobre el derecho a la reserva, el cual garantizará que no se pueda utilizar información relativa al pensamiento político y, no solo, a la filiación política. Así también evidenciamos una reformulación, en cuanto, al derecho a la protección de datos, estableciéndose el derecho a acceder y decidir sobre información y datos de carácter personal y a que estos sean protegidos; además, de que para la recolección, archivo, procesamiento, distribución o difusión de esos datos se requerirá la autorización del titular o la prescripción de la Ley cuando sea pertinente.

[241] En la votación, sobre el artículo 1 de los derechos civiles, con la presencia de noventa y cuatro asambleístas se obtuvo: Setenta y tres afirmativos; cinco negativos; cero blancos y dieciséis abstenciones.

legislador cuente con criterios jurídicos razonables, que faciliten la adaptación del derecho a la protección de datos personales en el régimen secundario.

Como veremos más adelante, la Ley Orgánica de Protección de Datos Personales, aprobada en mayo de 2021, requiere que el legislador tenga los conocimientos necesarios, sobre temas relativos al derecho a la protección de datos personales. Sin embargo, reiteramos que este derecho fundamental se enmarca dentro de un Estado constitucional de derechos y justicia. Así, tomando en cuenta que bajo este paradigma se establecen "fines, que son la realización de los derechos fundamentales, y medios, que son los poderes públicos y sus mecanismos de actuación"[242], los derechos fundamentales establecidos en la Constitución se desarrollan sobre la base de una nueva forma de Estado, que difiere del positivismo legalista de otras épocas, por ejemplo, el planteado en la Constitución de 1998. Por tanto:

> La clave está en distinguir la diferencia entre un estado legal y un estado constitucional. En el estado legal, la autoridad estaba sometida a la Ley y la Ley es hecha por el Parlamento; el Parlamento al elaborar la Ley resultaba ser la única autoridad no sometida. En el estado constitucional, en cambio, toda autoridad, incluida el parlamento, está sometida a la Constitución. Pero la Constitución tampoco es cualquier norma: tiene derechos que se consideran fundamentales[243].

Justamente, como precisa la CCE, nos referimos a la teoría neoconstitucionalista que desarrolla una nueva forma de Estado caracterizada por: "1) El reconocimiento del carácter normativo Superior de la Constitución; 2) La aplicación directa de la Constitución como norma jurídica; y 3) El reconocimiento de la jurisprudencia constitucional como fuente primaria de derecho"[244]. De tal forma que, "la consecuencia práctica de que la Constitución sea fuente del derecho sin más, es que aquellos temas fundamentales del ordenamiento jurídico, que en el paradigma

[242] Ávila Santamaría, *El Neoconstitucionalismo andino,* 61.
[243] Ibíd., 57.
[244] Véase el Registro Oficial Suplemento 451 de 22 de octubre del 2008. Corte Constitucional del Ecuador. (2008). Resolución S/N.

del Estado liberal eran materia de la Ley, ahora, en el paradigma de la constitucionalidad, son regulados directamente por la Constitución"[245].

Ante las posibles deficiencias del nuevo marco normativo de protección de datos personales en Ecuador o vacíos jurídicos –a condición de que sean, debidamente, reglamentados–[246]; planteamos que el reconocimiento constitucional de este derecho supone la exigencia de aplicar la Constitución como una regla de decisión. Naturalmente, frente a cualquier norma sectorial que se le contraponga prevalecerá el carácter supremo de la Constitución[247]. Además, siendo la normativa constitucional de aplicación directa como norma jurídica, impone a cualquier funcionario público la aplicación directa e inmediata de los derechos y garantías reconocidos, no solamente en la Constitución sino también en la jurisprudencia constitucional y en los instrumentos internacionales de derechos humanos[248].

### 7.4 La Corte Constitucional en la definición del derecho fundamental a la protección de datos: precisiones sobre los derechos de acceso, rectificación, cancelación y oposición

Ha transcurrido más de una década desde el reconocimiento constitucional del derecho fundamental a la protección de datos y los precedentes jurisprudenciales, a pesar de seguir siendo escasos, han sido importantes para los fines de la

[245] Ibíd.

[246] Debemos destacar que han sido tres los proyectos de Ley que –en 2010, 2016 y 2019– promovieron la articulación de un marco adecuado y propicio para la regulación y protección del derecho a la autodeterminación informativa. Esto es fundamental ya que, como queda evidenciado, el Estado constitucional de derechos y justicia exige la concreción de normas jurídicas claras con el objeto de asegurar el derecho a la seguridad jurídica de los ciudadanos.

[247] En todo caso, señalamos que la existencia de una Ley General de protección de datos garantiza el derecho a la seguridad jurídica, el cual significa un derecho sustancial en el Estado constitucional de derechos y justicia.

[248] Puede afirmarse que el reconocimiento constitucional en Ecuador se asemeja, por ejemplo, al derecho fundamental contemplado en la Carta de Derechos Fundamentales de la Unión Europea, en su art. 8. Ambos textos reconocen el derecho a la protección de datos de carácter personal; las facultades de control sobre el tratamiento de la información y el consentimiento como base del tratamiento. En todo caso, a diferencia de la Carta de Derechos Fundamentales de la Unión Europea, el texto constitucional ecuatoriano carece del reconocimiento de una autoridad de control independiente que garantice el respeto de este derecho.

protección de la información de carácter personal. Desde la jurisprudencia constitucional, tanto el derecho a la intimidad, como la garantía del *habeas data,* plantearon importantes supuestos para la garantía de este derecho.

Considerándose con toda seguridad como la primera sobre la materia, la Resolución Nro. 28 de 2001 de la CCE reconoció que la garantía del *habeas data* se concibe como un derecho a "guardar y preservar la intimidad, el honor y la honra del buen nombre, la buena reputación, la inviolabilidad de la correspondencia, papeles privados, derechos intelectuales"[249]. Así también la CCE ha señalado que la institucionalización de esta garantía en el Derecho Constitucional Latinoamericano se origina, a partir del desarrollo y expansión de las tecnologías, y que, por tanto, se orienta a impedir que terceros causen daño, afecten al honor y utilicen de manera maliciosa la información personal de los interesados[250].

Se trata de un precedente importante en materia de protección de datos, por cuanto garantiza la tutela de la intimidad e inviolabilidad de la correspondencia y papeles privados. A esto, se suma la garantía de los derechos –sobre todo aquellos ligados a la dignidad de la persona– que se desprenden de la expansión del paradigma informático. Precisamente, como ha señalado la doctrina, estimar al derecho fundamental a la protección de datos "como un derecho autónomo o instrumental del derecho a la intimidad no debe hacernos olvidar que ambos derechos poseen el mismo origen: la dignidad de la persona"[251].

A partir de la Resolución Nro. 28 de la CCE, existen otros precedentes que intentaron desarrollar el derecho a la protección de datos, mediante el concepto de intimidad y *habeas data*[252]. Naturalmente, esto ocurrió antes de que la Constitución de 2008 reconociera a la protección de datos como un derecho autónomo. Por

[249] Véase el Registro Oficial Suplemento 281 de 9 de marzo del 2001 (caso signado con el Nro. 39-2000-HD).
[250] Ibíd.
[251] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 37**.**
[252] Por ejemplo, puede citarse las siguientes Resoluciones del Tribunal Constitucional: Nro. 12 –Caso Nro. 12-2002-HD–; la Resolución Nro. 46 –Caso Nro. 46-2002-HD–; la Resolución Nro. 26 –Caso Nro. 26-2003-HD–; la Resolución Nro. 20 –Caso Nro. 20-2004-HD– y la Resolución Nro. 76 –Caso Nro. 76-2004-HD–.

ejemplo, respecto al *habeas data*, la Resolución Nro. 46 de 2002 de la CCE precisa que esta garantía permite acceder al titular de los datos personales a los archivos públicos o privados, "en los cuales están incluidos sus datos personales o de su familia, para requerir su rectificación o la supresión de aquellos datos inexactos que de algún modo le pudiesen perjudicar en su honra, buena reputación e intimidad"[253].

Si bien a la fecha de expedición de esta última Resolución, el derecho a la protección de datos no se encontraba reconocido en la Constitución, la CCE señalaba que:

> El derecho a la protección de datos implica, a su vez, el derecho a conocer la existencia de ficheros o de información almacenada y el propósito o la finalidad que se persigue con ellos; el derecho a acceder, que permite a los afectados averiguar el contenido de la información registrada, o participar de la información que sobre la imagen o concepto de ellos se tenga; y el derecho a rectificar, que es la posibilidad del titular afectado, de que los datos sobre su persona o de su entorno familiar al ser incorrectos, inexactos u obsoletos, sean rectificados en la medida en que, al ser ajenos a la realidad, le pueden causar perjuicio a su familia o a sus bienes.

Ahora bien, a partir, del reconocimiento constitucional en la Carta Magna de 2008, el desarrollo del derecho fundamental a la protección de datos en la jurisprudencia constitucional ha sido, relativamente, significativo en relación a su reconocimiento como un derecho autónomo e independiente y que comparte con el *habeas data* las facultades de garantía, control y dominio sobre la información personal. Así, son tres Resoluciones las que se destacan. La Resolución Nro. 19-9-SEP-CC, la Nro. 1-14-PJP-CC y la Nro. 182-15-SEP-CC de la CCE instituyen las bases para la protección de este derecho fundamental, dentro del Estado constitucional de derechos y justicia[254].

En lo medular, la Resolución Nro. 19-9-SEP precisa que el *habeas data*:

> Protege a la integridad moral de las personas frente a informaciones referidas a su personalidad, tales como: su afiliación política, gremial, religiosa, su historia laboral, sus antecedentes crediticios, policiales e informaciones similares que constan en registros o bancos de datos (…) Así concebido y entendido el hábeas data, no se trata de una acción procesal civil, sino de una garantía constitucional con objetivos muy precisos, que busca que el accionante sepa: 1) Cuáles son los motivos legales por los que el poseedor de la información llegó a ser tenedor de la misma; 2) Desde cuándo tiene la información; 3) Qué

[253] Véase el Registro Oficial Suplemento 66 de 22 de abril de 2003 –Caso signado con el Nro. 46-2002-HD–.

[254] Debe considerarse que la Resolución 1-14-PJP-CC de la CCE constituye un precedente jurisprudencial vinculante respecto a los casos relacionados en la materia.

> uso se ha dado a esa información y qué se hará con ella en el futuro; 4) Conocer a qué personas naturales o jurídicas, el poseedor de la información hizo llegar la misma; por qué motivo, con qué propósito y la fecha en la que circuló la información; 5) Qué tecnología usa para almacenar la información; y 6) Qué seguridades ofrece el tenedor de la información para precautelar que la misma no sea usada indebidamente[255].

Como sabemos, el uso de las tecnologías de la información y comunicación es una de las características del Siglo XXI. Ecuador por mandato constitucional garantiza que toda persona, en forma individual o colectiva, tiene derecho al "acceso universal a las tecnologías de información y comunicación" –art. 16.2–. No obstante, advertimos que el uso ilícito de estas tecnologías representa serios riesgos en la protección de los datos personales[256]. Por tanto, la posibilidad de contar con una normativa de protección de datos sugiere establecer un modelo de garantía, no solamente respecto a este derecho fundamental sino también un ordenamiento jurídico que respete, integralmente, otros derechos fundamentales como los derechos digitales de las personas. Al parecer, en los últimos años, uno de los principales objetivos del Estado ecuatoriano ha sido incrementar en la población el acceso y uso de las tecnologías de la información y comunicación, olvidando con ello estimar los riesgos que se desprenden del uso de las tecnologías[257]. Si bien el

[255] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –Caso Nro. 14-9-EP– publicada en el Registro Oficial 18 de 3 de septiembre de 2009.

[256] Por ejemplo, en el contexto internacional, la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales de España ha incorporado en la normativa de protección de datos la regulación de derechos digitales. Así, en el preámbulo de la Ley Orgánica 3/2018 se destaca que "el Título X de esta Ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital, así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales".

[257] Con respecto al uso del Internet por parte de las personas a nivel nacional, el 15 de junio de 2017 el Gobierno de la República del Ecuador expidió, mediante Acuerdo 11-2017 las "Políticas Publicas del Sector de las Telecomunicaciones y de la Sociedad de la Información 2017-2021", sustentados en dos ejes relacionados con el despliegue de la infraestructura de las telecomunicaciones y fomento de proyectos de carácter social y de ampliación del servicio universal de telecomunicaciones. Esta política menciona que, a partir, de la definición y ejecución de políticas públicas en el sector de las telecomunicaciones, existe un importante crecimiento en los últimos años tomando en consideración que para el 2010 el 29% de la población utilizó Internet y para el 2015 el 51%.

acceso a las tecnologías e Internet se consideran como un derecho fundamental, es necesario también estimar los elementos que deben converger para la protección integral del derecho a la protección de datos, en el entorno digital[258].

En este orden de ideas, la Resolución 19-9-SEP-CC aclara que el *habeas data* garantiza acceder "y verificar la información y, como consecuencia, pedir que se actualicen los datos, rectificarlos o anularlos si fueren erróneos o afecten a nuestros derechos, fundamentalmente a nuestra honra o intimidad"[259]. Por ello, hay que recordar que esta garantía, en una sociedad digital, se orienta a "conocer a qué personas públicas o privadas, naturales o jurídicas, el titular de los archivos o bases de datos, transmitió informaciones personales referentes al sujeto que ejercita la acción"[260]. Naturalmente, frente a ese conocimiento, el *habeas data* permite ejercer la facultad de "comprobar si la información es actualizada y correcta y, de no serlo, solicitar y obtener su actualización o rectificación"[261]. Por consiguiente, se pretende tutelar el control de la forma en la que se recopilan, almacenan y utilizan sus datos personales. En suma, ejercer la facultad de "solicitar la cancelación de los datos personales si no corresponde su almacenamiento a la finalidad que legítima su registro"[262].

Por otra parte, la Resolución Nro. 1-14-PJP-CC de la CCE –como se verá más adelante– se dedica, expresamente, a fijar algunas reglas jurisprudenciales vinculantes sobre los derechos que corresponden a los titulares de los datos personales[263]. Así, respecto al derecho a la autodeterminación informativa, la CCE

---

[258] En todo caso, la Guía Legislativa de la OEA destaca que "Las normas relativas a la privacidad deben permitir que los consumidores y las empresas se beneficien del uso de datos personales de una manera segura y protegida. Deben ser equilibradas y tecnológicamente neutrales y permitir el libre flujo de datos dentro de cada país y a través de fronteras nacionales de una manera que fomente la innovación tecnológica y promueva el desarrollo económico y el crecimiento del comercio".

[259] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –Caso Nro. 14-9-EP– publicada en el Registro Oficial 18 de 3 de septiembre de 2009.

[260] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*,119.

[261] Ibíd.

[262] Ibíd.

[263] En la fundamentación de las reglas jurisprudenciales, la CCE ha señalado que "el derecho a la protección de datos –y específicamente, su elemento denominado "autodeterminación informativa–", tiene un carácter instrumental, supeditado a la protección de otros derechos constitucionales que

señala que este derecho implica "la posibilidad de que dentro de los límites que franquean la Constitución y la Ley, se tenga capacidad para ejercer cierto control sobre el uso que se haga de tal información, aunque el poseedor de la misma sea otra persona"[264]. De este modo, recalcamos que estas facultades "se ejercen no sólo frente a responsables de ficheros públicos, sino también frente a responsables privados, por lo que se trata de un derecho fundamental que se desarrolla también entre particulares"[265]. Por ello, se advierte que el respeto del derecho a la protección de datos se encuentra sujeto al cumplimiento de ciertas obligaciones que deben cumplir las organizaciones, tanto dentro del ámbito público como privado[266].

Finalmente, otra Resolución importante es la Nro. 182-15-SEP-CC. En primer término, en este precedente de la CCE precisa que los derechos y garantías reconocidos en los arts. 66.19 y 92 de la Constitución tienen un "carácter autónomo, por cuanto posee un perfil propio regulado tanto en la Constitución como en la Ley de la materia y tutela datos o información inherente a una persona, a fin de salvaguardar su derecho a la intimidad personal y familiar"[267]. Luego de atribuir su autonomía, como un derecho fundamental a la protección de datos, también define al *habeas data* como una acción constitucional que posee una órbita específica "esto es, la información íntima de una persona, la cual puede estar contenida en diversas formas, tales como documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, repose en custodia de personas naturales o jurídicas públicas o privadas, ya sea en soporte material o electrónico". Además, como se analizará en otro momento, esta

se pueden ver afectados cuando se utilizan datos personales, como puede ser la intimidad, la honra, la integridad psicológica, etc.".

[264] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –Caso Nro. 67-11-JD– publicada en el Registro Oficial Suplemento 281 de 3 de julio de 2014.

[265] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 548.

[266] Con referencia a este aspecto, la CCE agrega que "si bien, originariamente, el habeas data se había perfilado como una garantía de acceso a los datos personales, con el tiempo se empezó a aplicar, por extensión, respecto de los datos en poder de la Administración con fines de esclarecimiento de la actividad realizada por los gobernantes". Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –Caso Nro. 67-11-JD– publicada en el Registro Oficial Suplemento 281 de 3 de julio de 2014.

[267] Véase la Resolución de la Corte Constitucional 182, Sentencia Nro. 182-15-SEP-CC –Caso Nro. 1493-10-EP– publicada en el Registro Oficial Suplemento 607 de 14 de octubre de 2015.

Resolución de la CCE advierte que el *habeas data* se caracteriza por tener unas dimensiones utilitarias: *habeas data* informativo; *habeas data* aditivo; *habeas data* correctivo; *habeas data* cancelatorio; y *habeas data* de reserva[268].

Bajo estas consideraciones, es destacable la actividad desarrollada por la CCE, a partir del reconocimiento constitucional en la Carta Magna de 2008. No obstante, en la práctica, la garantía del derecho fundamental a la protección de datos requiere mucho más. Como señala nuestra Constitución, –respetando el derecho a la seguridad jurídica–, los derechos fundamentales, no solamente deben desarrollarse en la jurisprudencia sino también en la normativa y/o legislación secundaria, y a través, de políticas públicas. Entre otros problemas que se deben solucionar, a partir de la nueva normativa de protección de datos, encontramos "el desconocimiento que la mayor parte de las personas tienen sobre los peligros derivados del acceso por terceros a los datos que les identifican o permiten identificarlos cuando no afectan directamente a su vida íntima"[269]. Por ello, hay que enfatizar en la necesidad de concientizar en la Administración Pública y particulares, mediante políticas públicas sobre un manejo responsable de la información personal, el cual garantice los principios y derechos que se desprenden de la legislación de protección de datos.

### 7.5 Algunas precisiones finales sobre el derecho fundamental a la protección de datos personales. Referencia a los artículos 66.19 y 92 de la Constitución ecuatoriana

En el derecho constitucional ecuatoriano, la protección de datos personales se ha desarrollado en tres etapas: primero, la protección constitucional, a través, del *habeas data;* segundo, la regulación de la información personal y la intimidad mediante Leyes sectoriales; y tercero, el reconocimiento de un derecho fundamental

[268] Ibíd. Si bien estas dimensiones se describen en la Sentencia 182-15-SEP-CC, la primera referencia a esta clasificación se la hizo en la Sentencia Nro. 25-15-SEP-CC. Al respecto, Véase el Registro Oficial Suplemento 485 de 22 de abril de 2015 –Caso signado con el Nro. 725-12-EP–.
[269] Pablo Lucas Murillo de la Cueva, "La protección de los datos de carácter personal en el horizonte de 2010", *Anuario Facultad de Derecho – Universidad de Alcalá* Navarra, Nro. II (2009):131-142.

a la protección de datos personales en la Constitución de 2008. En todo caso, a partir de la promulgación de la Ley Orgánica de Protección de Datos de 2021, nos encontramos atravesando por una cuarta etapa.

En la Constitución de 2008, el derecho a la protección de datos personales se sitúa dentro de los denominados "derechos de libertad". Así, en relación a la Constitución de 1998, el actual ordenamiento constitucional elimina "la clásica división de derechos civiles, políticos, y económicos, sociales y culturales. En su lugar utiliza una división puramente temática (derechos de participación, derechos de libertad, etc.)"[270]. De esta manera, la Constitución reconoce y garantiza:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley –art. 66.19–.

A propósito de este derecho fundamental, dentro del modelo neoconstitucional que plantea el Estado ecuatoriano, su reconocimiento garantiza a todas las personas la "inviolabilidad de la intimidad personal o familiar y cualquier dato que forme parte de esa intimidad o que conciernen a su identidad, así como lo que dice relación a su honor, buen nombre o fama, reserva sobre sus convicciones religiosas, políticas, etc.,"[271]. Asimismo, la Constitución garantiza la tutela de este derecho fundamental, mediante el *habeas data* –art. 92–. En consecuencia, se garantizan "derechos del titular de los datos ante los responsables de los bancos, la acción o facultad para acudir a los jueces en defensa de estos derechos y, por último, el proceso en el que

[270] Agustín Grijalva, *Constitucionalismo en Ecuador*, (Quito-Ecuador: Corte Constitucional para el Período de Transición, 2012), 28. Para ilustrar mejor, la Constitución de 1998 consideraba derechos civiles los reconocidos en el artículo 23. Por ejemplo, en el numeral 8 el derecho a la honra, a la buena reputación y a la intimidad personal y familiar; numeral 13 la inviolabilidad y el secreto de la correspondencia; numeral 21 el derecho a guardar reserva sobre convicciones políticas y religiosas; y numeral 24 el derecho a la identidad. Mientras que la Constitución de 2008 considera como derechos de libertad los reconocidos en el artículo 66. Por ejemplo, en el numeral 19, el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección y numeral 20, el derecho a la intimidad personal y familiar.

[271] Julio Cesar Trujillo, "Las Garantías Jurisdiccionales", Recuperado de: Base de datos: Vlex.com.ec: https://app.vlex.com/#WW/vid/515951146/graphical_version.

se sustancia la acción"[272]. Situándose como una garantía jurisdiccional, la Constitución reconoce que:

> Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la Ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la Ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados –art. 92–[273].

Conforme a la normativa constitucional citada, el *habeas data* concentra las facultades de control y dominio sobre el tratamiento de la información de carácter personal, tanto el ámbito público como privado. Se destaca el reconocimiento de los principios de finalidad; licitud; uso limitado; retención (tiempo de vigencia del archivo o banco de datos); transparencia y consentimiento en la recogida de datos, así como

[272] Ibíd., 269.

[273] Conviene señalar que, la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional de Ecuador orientada a "garantizar jurisdiccionalmente los derechos reconocidos en la Constitución y en los instrumentos internacionales de derechos humanos" –art. 1–, reconoce que la acción de habeas data tiene por objeto: "garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos. El titular de los datos podrá solicitar al responsable del archivo o banco de datos, el acceso sin costo a la información antes referida, así como la actualización de los datos, su rectificación, eliminación o anulación. No podrá solicitarse la eliminación de datos personales que por disposición de la Ley deban mantenerse en archivos públicos. Las personas responsables de los bancos o archivos de datos personales únicamente podrán difundir la información archivada con autorización del titular o de la Ley. Las presentes disposiciones son aplicables a los casos de rectificación a que están obligados los medios de comunicación, de conformidad con la Constitución. El concepto de reparación integral incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación" –art. 49–. Adicionalmente, respecto al ámbito de protección de la acción de *habeas data,* esta misma Ley dispone que esta acción procede cuando: "1. Cuando se niega el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o estén en poder de personas naturales o jurídicas privadas. 2. Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos. 3. Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente" –art.50–.

la protección y seguridad de los datos sensibles. Desde esta perspectiva, el *habeas data* asegura la garantía y ejercicio de los derechos de acceso, rectificación, eliminación o anulación de los datos personales que consten, tanto en soporte material como electrónico. Además, al determinarse que esta garantía procede cuando "se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa", existe un reconocimiento de que el derecho fundamental a la protección de datos personales es un instituto de garantía de otros derechos fundamentales.

Sobre este respecto, reiteramos que:

> La dimensión teleológica del *habeas data* se cifra en proteger a los titulares de esa acción procesal contra la invasión de su intimidad, en su acepción más amplia que abarca también a todos los aspectos de la vida privada, del honor y de la imagen de las personas concernidas. Se trata, en definitiva, de una acción dirigida a conocer, acceder, rectificar, suprimir y prohibir la divulgación de determinados datos, ya sea porque han sido indebidamente procesados o porque se pretenda utilizarlos o transmitirlos al margen de la finalidad que legitimaba su registro[274].

En todo caso, la doctrina ecuatoriana también advierte que:

> La Constitución ecuatoriana (art. 92) y la LOGJCC (art. 49) reconoce al titular el derecho para demandar la reparación de los perjuicios que le haya irrogado con el banco de datos, por la violación de cualquiera de las normas que regulan la elaboración de los bancos de datos personales, la protección de los derechos de la persona y, en general, cualquier otro derecho legalmente garantizado y la reparación debe ser integral o de los daños económicos o patrimoniales, el daño moral, el buen nombre o fama, la garantía de que no se volverán a repetir violaciones análogas, etc.[275].

Bajo estas consideraciones, el paradigma del Estado constitucional de derechos y justicia supone una manifiesta universalización de los derechos concretados en las garantías constitucionales, particularmente, del derecho fundamental a la protección de datos personales. Como apunta Grijalva:

> Esta universalización de la capacidad para reclamar derechos se corrobora también en una ampliación y desarrollo de las garantías constitucionales. Las garantías en sentido amplio son los medios de los que disponen los ciudadanos para hacer efectivos sus derechos constitucionales. La Constitución de 2008 amplia y fortalece estas garantías[276].

[274] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 119-120.
[275] Trujillo, "Las Garantías Jurisdiccionales", 270.
[276] Agustín Grijalva, *Constitucionalismo en Ecuador*, 29.

La ampliación y desarrollo de la garantía de *habeas data,* –a partir de lo que señala Grijalva–, surge como resultado de aquella universalización que plantea la libertad informática, en una sociedad en la que predomina el avance tecnológico y comercial. En este sentido, agregamos que:

> Una vez que el Estado social y democrático o de derechos y justicia tiene como deber primordial respetar y hacer respetar los derechos de la persona y garantizar la seguridad integral o humana, la persona tiene derecho para demandar del Estado ecuatoriano la protección de su libertad informática o informativa y a que arbitre las medidas para impedir el abuso del poder informático como de cualquier otra forma de poder, como lo hace, desde las revoluciones del siglo XVIII, frente al poder político del mismo Estado[277].

Por tanto, a la luz de la teoría del Estado constitucional en Ecuador, es importante considerar la naturaleza y el alcance que tiene el derecho fundamental a la protección de datos y garantía de *habeas data.* En este aspecto, Grijalva precisa que:

> Se completa y perfecciona el procedimiento de la acción de *habeas data* establecido de forma más general en la Constitución de 1998. Para este efecto, se incluye como objeto del *habeas data* los datos genéticos y los archivos de datos personales; se aclara que la acción puede interponerse sin importar si la información se halla en forma electrónica o manual. El titular tiene derecho a conocer la finalidad, propósito, origen y destino de su información personal. Si los datos son sensibles, el titular podrá pedir que se adopten medidas de seguridad adecuadas[278].

Por otra parte, considerando que la Constitución prescribe –como un principio para la aplicación de los derechos– que el contenido de los derechos se desarrollará de manera progresiva en las normas, jurisprudencia y políticas públicas –art. 11.8–; se espera que la nueva normativa aprobada materialice la formulación de políticas públicas[279], por cuanto desde la significación de este derecho fundamental en el contexto internacional, esta Ley general debe responder a las exigencias que plantea el derecho a la protección de datos.

---

[277] Trujillo, "Las Garantías Jurisdiccionales", 262.

[278] Ibíd., 254.

[279] Si bien han sido tres los proyectos que, históricamente, se han presentado ante el legislativo, en los últimos años, solo dos han despertado especial interés en la materia. El primero, denominado "Proyecto de Ley Orgánica de la protección de los Derechos a la Intimidad y Privacidad sobre los datos personales", presentado en 2016 y el segundo, denominado "Proyecto de Ley Orgánica de Protección de Datos Personales" formulado en 2019. Este último que, finalmente, ha concretado su aprobación y promulgación en el Registro Oficial. Puede consultarse el texto completo de ambos proyectos en el Portal de la Asamblea Nacional del Ecuador: https://Leyes.asambleanacional.gob.ec/.

Como se analizará en los siguientes capítulos, es necesario que la ley aprobada recoja, principalmente, las recomendaciones regionales que se plantean, tanto en la Guía Legislativa de la OEA como en los Estándares de protección de datos personales para los Estados Iberoamericanos. En todo caso, también será esencial precisar las garantías que en la actualidad dispone el RGPD, con el objeto de alcanzar un nivel adecuado de protección, acorde a estándares internacionales. Así, entendemos que la realidad ecuatoriana debe adecuarse a los estándares que, internacionalmente, plantea la protección de datos personales, por cuanto contar con estándares comunes "con un alcance global acerca de la protección de datos personales no solo es necesaria sino también posible, toda vez que sus cimientos ya han sido establecidos por el propio reconocimiento y desarrollo del derecho a la vida privada"[280].

En este contexto, debe garantizarse que este derecho fundamental se desarrolle acorde a planteamientos globales. Buscando el bienestar colectivo de la sociedad, debe posibilitarse la protección integral de la dignidad de la persona, frente a los procesos de desarrollo tecnológico y comercial. Desde esta perspectiva, el modelo europeo representa una experiencia palpable de integración para la protección de este derecho fundamental[281]. Por ello, la aplicación de estándares comunes es un presupuesto que debe asumirse en el país y en la región con el objeto de establecer un modelo de protección de datos personales a escala internacional.

Finalmente, siguiendo a Puccinelli, conviene resaltar que:

[280] María Maqueo Ramírez, Jimena Moreno y Miguel Recio Gayo, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", *Revista de Derecho (Valdivia)*, Nro. 1 (2017), 94.

[281] Como señala Antonio Troncoso: "Hay que tener en cuenta que pocos derechos son tan importantes para la construcción y para hacer viable ese espacio común que hoy representa la Unión Europea como el derecho fundamental a la protección de datos personales. Si el objetivo clásico de la Unión Europea era la libre circulación de personas, mercancías y capitales, y, por tanto, de datos personales, este movimiento solo era posible si los países que la componen disponían de un modelo de protección de datos personales homogéneo. Se hacía necesario, pues, el establecimiento de un sistema de protección de datos a escala europea que habilitara el intercambio de información personal mediante el establecimiento de estándares comunes. Cfr. Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 36-37.

> A fin de abordar correctamente la cuestión, un primer aspecto que debe considerarse especialmente es tener clara la distinción que debe hacerse entre el derecho a la protección de datos, la acción de *habeas data* y el proceso de *habeas data*, pues de aquel se desprenden las facultades que la acción intenta tutelar a través de este último cuando esa tutela es urgente[282].

Para este fin, la Resolución Nro. 1-14-PJP-CC de la CCE –constituida como el primer precedente jurisprudencial de carácter obligatorio– singulariza, tanto al derecho fundamental a la protección de datos personales como al *habeas data*[283]. Esta Resolución desarrolla seis reglas, a partir de tres momentos o problemas que resuelve la Corte[284].

El primer problema que plantea la Corte es: ¿Puede considerarse a una persona jurídica como titular de los derechos protegidos por medio de la acción de *habeas data*? En este caso, las tres primeras reglas señalan:

1. La determinación respecto de si una persona jurídica puede beneficiarse de una provisión constitucional que contenga un derecho constitucional debe hacerse caso por caso, en consideración de las posibilidades derivadas de su naturaleza social, así como de los términos en los que está formulado el derecho en la Norma Constitucional.

2. En el caso de la autodeterminación informativa, como parte del derecho a la protección de datos personales, implica la necesidad de garantizar la protección de la esfera íntima de las personas, así como la posibilidad de ejercer control sobre los datos personales del sujeto, aunque no se encuentren en su poder.

3. Por las características del derecho a la protección de datos personales, no se considera constitucionalmente adecuada la limitación a la calidad de las personas jurídicas como titulares del mismo; sin embargo, la información personal de dichos sujetos únicamente se extiende a las personas asociadas o a sus representantes legales, en tanto a la calidad que ostentan respecto de la persona jurídica, con estricto respeto al derecho a la protección de los datos personales y derechos conexos que le son atinentes a su naturaleza.

El segundo problema que se plantea es: ¿Quién ejerce la legitimación activa para reclamar la tutela de derechos protegidos por medio de la acción de *habeas data* de las personas jurídicas? A este respecto, se señalan dos reglas:

---

[282] Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de *habeas data* a dos décadas de su creación", 815.

[283] Como dispone la CCE, esta Resolución "tendrá efectos generales hacia el futuro, respecto de todos los casos en donde se interpongan acciones de garantía jurisdiccional de los derechos constitucionales y se verifiquen los supuestos de esta sentencia, sin perjuicio de que se aplique también este precedente jurisprudencial a casos en los que ya se hallen en trámite dichas garantías".

[284] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –Caso Nro. 67-11-JD– publicada en el Registro Oficial Suplemento 281 de 3 de julio de 2014.

4. La legitimación activa para la presentación de la acción de *habeas data* requerirá que quien lo haga sea el titular del derecho a la protección de datos personales que se alegue vulnerada, o su representante legitimado para el efecto.

5. Para acreditar la representación de las personas jurídicas será suficiente la entrega del documento que la Ley que regule la materia determine como suficiente para considerar iniciadas sus funciones como representante. El juez constitucional, una vez acreditada la representación, deberá tramitar la acción sin que medie excepción sobre el cumplimiento de los requisitos de Ley respecto del documento entregado, lo que deberá ser dilucidado por los organismos competentes en sede ordinaria.

El tercer problema planteado formula: ¿Es la entrega física de documentos originales parte de las finalidades perseguidas por medio de la acción de *habeas data*? La última regla señala:

6. El *habeas data*, como mecanismo de garantía del derecho a la protección de datos personales, no podrá ser incoado como medio para requerir la entrega física del soporte material o electrónico de los documentos en los que se alegue está contenida la información personal del titular sino para conocer su existencia, tener acceso a él y ejercer los actos previstos en el artículo 92 de la Constitución de la República; el juez está obligado a utilizar todos los mecanismos que establece la Ley para efectos de garantizar debida y eficazmente los actos constantes en el artículo referido.

A pesar de la reciente data de esta Resolución, ya evidenciamos, anteriormente, que años atrás la misma CCE había resuelto sobre la naturaleza del derecho a la protección de datos y garantía de *habeas data*. Así, agregamos que la Resolución Nro. 19-9-SEP-CC conceptualizó su alcance y naturaleza[285]. Atendiendo a la CCE, ésta señala:

> En este sentido, el texto constitucional consagra al *habeas data* como un derecho fundamental en sí mismo, independiente de otros y como un mecanismo de protección de otros derechos fundamentales, como el derecho a la honra, al honor, a la intimidad, al buen nombre, a la imagen, a la verdad, al patrimonio, a la privacidad, a la voz y a la autodeterminación informativa frente al abuso y negligencia en el tratamiento de la información.

En estas condiciones, nos parece que uno de los méritos más importantes de la Constitución de 2008 es haber reconocido y atribuido autonomía al derecho fundamental a la protección de datos personales, reconociéndolo como un instituto de garantía de otros derechos fundamentales. En una sociedad tecnológica, la ampliación de la garantía de *habeas data* supone la obligación de adoptar las

[285] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –Caso Nro. 14-9-EP– publicada en el Registro Oficial 18 de 3 de septiembre de 2009.

medidas de seguridad necesarias para el tratamiento de los datos sensibles o especialmente protegidos.

A partir de la necesidad de proteger la información de carácter personal, como resultado de los avances tecnológicos experimentados en la sociedad, en Ecuador ha sido importante el aporte de la jurisprudencia constitucional respecto a la determinación de las bases del derecho a la protección de datos personales como un derecho fundamental. Es así que, desde la constitucionalización de este derecho, se aprecia un antes y un después en la regulación sectorial; y que ahora, ha permitido concretar la aprobación de una normativa que desarrolle el derecho a la protección de datos. Lógicamente, en los siguientes capítulos nos ocuparemos de analizar su correcta adecuación, a partir de los estándares de protección que exige la comunidad internacional.

## CAPÍTULO II: ESTUDIO COMPARADO DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES

### 1. Introducción

Con la evolución de la tecnología e integración comercial, la sociedad ha experimentado gran dificultad para garantizar la protección de bienes jurídicos, tradicionalmente, tutelados, a través del derecho a la intimidad que ahora requieren una tutela más específica y amplia que les proporcione el derecho a la protección de datos personales. Existen varias problemáticas derivadas de los avances tecnológicos y comercio internacional, que se traducen en necesidades al momento de garantizar este derecho fundamental, a partir del tratamiento de la información, sea en el ámbito público o privado[1].

Frente a la protección de datos, el desarrollo de las nuevas tecnologías y los procesos de integración comercial pueden desencadenar en situaciones que atentan contra los derechos de libertad. Y que se desprenden del instituto de garantía que tutela el derecho a la protección de datos. "Por ello, debe resaltarse con intensidad la importancia que ha de otorgarse a la protección de datos de carácter personal como derecho que favorece el ejercicio efectivo de la libertad"[2]. Precisamente, uno de los cambios más importantes que se derivan de estas problemáticas es el tratamiento de la información, desde medios impresos hacia la digitalización de la información personal. Así, destacamos que la libertad de "defender la privacidad informática individual se ha convertido también en libertad de comunicar a los demás las informaciones transmisibles por vía telemática, para ejercitar así la libertad de expresión de la propia personalidad sirviéndose de los

[1] Así, por ejemplo, advertimos que: "El aumento sustancial en los flujos transfronterizos de datos motivado en la mayor integración económica y social y el mayor intercambio entre operadores públicos y privados, con más el notorio incremento de la economía digital han generado un escenario en el que todos estos factores interactúan a tal punto que a veces se torna dificultoso establecer los límites entre ellos". Cfr. Valeria Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", *Revista Transparencia y Sociedad – Consejo para la Transparencia de Chile*, Nro. 5 (2017):13-31.

[2] Pablo Lucas Murillo de la Cueva y José Luis Piñar Mañas, El *derecho a la autodeterminación informativa* (Madrid-México: Fontamara S.A, 2011), 110**.**

sistemas de comunicación automatizados"[3]. En los ordenamientos jurídicos latinoamericanos y europeos, el proceso de constitucionalización de los derechos fundamentales de las personas incorporó, recientemente, un derecho autónomo a la protección de datos personales, frente a la necesidad de dar respuesta al proceso de evolución tecnológica. De igual manera, surgiría como un mecanismo que favoreciera a los procesos de integración económica y comercial.

Por otra parte, los escándalos de manipulación de datos de millones de usuarios de redes sociales y plataformas digitales dejan al descubierto una serie de interrogantes, respecto al marco transfronterizo de protección de la información de carácter personal. Atendiendo a esto, apuntamos que:

> Cada vez es más complicado determinar la jurisdicción competente –cuál es la legislación aplicable y la autoridad para resolver las disputas- y quien es el responsable del tratamiento. Las amenazas al derecho fundamental a la protección de datos personales provienen de más allá de las fronteras de la Unión Europea, lo que exige que, al menos, la normativa de protección de datos personales -y en el futuro las propias instituciones de tutela- tengan también un carácter supranacional[4].

Este escenario obliga a repensar un modelo de regulación global que permita proteger de manera integral este derecho fundamental. Así, por ejemplo, la Unión Europea y algunos organismos o instancias internacionales han desarrollado una serie de instrumentos, los cuales representan modelos de regulación y protección de la información personal, "tendentes a fortalecer la protección de la privacidad y de los datos personales, a la vez que buscan resguardar y equilibrar los demás derechos que confluyen en este esquema"[5].

No obstante, el problema sigue siendo, en nuestro ámbito territorial, la integración latinoamericana –y comunitaria andina– debido a la múltiple y heterogénea variedad de modelos jurídicos. En el contexto latinoamericano, al igual que en otras áreas geográficas, la protección de datos personales se ha derivado de la necesidad de salvaguardar los derechos o libertades personales que pueden ser afectadas, en

[3] Tommaso Edoardo Frosini, "Nuevas tecnologías y constitucionalismo", *Revista Derecho del Estado*, Nro. 15 (2003): 29-43.
[4] Antonio Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, Nro. 43 (2012): 25-184.
[5] Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", 18.

virtud del tratamiento de la información personal, principalmente, como resultado de la incorporación de procesos tecnológicos en el tratamiento de la información.

A esto, se suma la gran influencia que ejercen los procesos de integración económica y comercial que han obligado a los estados latinoamericanos a desarrollar niveles adecuados de protección. Lógicamente, la influencia del modelo europeo es una de las características que en algunos países de Latinoamérica y de la Comunidad Andina han permitido implementar mecanismos de protección, de tutela, de supervisión y control.

En este aspecto, destacamos que:

> Esta aproximación de los países iberoamericanos al modelo europeo de protección de datos personales está siendo valorada positivamente por la Comisión Europea, a través del reconocimiento de que estos países tienen un nivel adecuado de protección –que ha obtenido hasta ahora Argentina en 2003 y Uruguay en 2112–. Este reconocimiento abre la posibilidad de que los países iberoamericanos se conviertan en un espacio donde sean posibles inversiones y actividades empresariales que impliquen transferencias de datos personales, convirtiendo esa región en un espacio más competitivo para el ámbito de las TIC[6].

La satisfacción del interés común y de la seguridad jurídica, en lo que respecta a la protección de la información personal, frente a estos avances y exigencias que se plantean, comporta que este derecho fundamental ponga "en manos de los interesados instrumentos que les permitan recuperar, al menos en parte, el control sobre la información personal que les concierne y que está o puede estar en manos de terceros"[7]. Naturalmente, sobre la base del desarrollo tecnológico y la necesidad de incrementar los intercambios comerciales, "los operadores económicos requieren de una mayor seguridad jurídica que permita las transferencias de datos personales a través de las fronteras interiores de la UE, algo incompatible con la actual fragmentación de las legislaciones nacionales."[8]. Por estas razones,

[6] Antonio Troncoso, "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional", *Revista Latinoamericana de Protección de Datos Personales*, Nro. 5 (2012). Disponible en: https://tinyurl.com/rvtguwp

[7] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 16.

[8] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 70.

consideramos imprescindible analizar el contexto internacional que desarrolla la tutela del derecho fundamental a la protección de datos.

En América Latina algunas reformas constitucionales "introdujeron la protección de los datos personales (algunas bajo la forma de *habeas data*), viz. Brasil (1988) artículo 5o.- X, Xll y LXXll; artículo 105 l b); Colombia (1991) artículo 15; Paraguay (1992) artículos 33, 36 y 135; Perú (1993) artículos 2o., 162, 203-3; Argentina (1994) artículos 19 y 43; y Ecuador (1998) artículos 23.8, 23.13, 23.24, 94"[9]. En el caso de Ecuador, recordemos que la protección de datos no se encontraba reconocida, en la Constitución de 1998, como un derecho fundamental. Su tutela se ejercía, a través de otros derechos fundamentales como el derecho a la honra, a la buena reputación y a la intimidad personal y familiar –art. 23.8–; derecho a la inviolabilidad y el secreto de la correspondencia –art. 23.13–; derecho a guardar reserva de convicciones políticas y religiosas –art. 23.21–; derecho a la identidad –art. 23.24–; y del *habeas data* –art. 94– como una garantía constitucional de protección[10].

Tomando como ejemplo el caso ecuatoriano, puede decirse que "de las iniciales elaboraciones teóricas que buscaban extender los confines del derecho a la intimidad a toda información personal, se pasó a identificar un bien jurídico autónomo –denominado intimidad informativa, *privacy*, libertad informática o autodeterminación informativa–"[11]. Precisamente, una muestra de aquello es el reconocimiento en la Constitución de 2008 del derecho fundamental a la protección

[9] Carlos Gregorio, "Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina", en Raúl Márquez Romero (coord.), *Transparentar al Estado: La experiencia mexicana de acceso a la información,* (México: Instituto de Investigaciones Jurídicas, 2005), 310-311.

[10] De las consideraciones que expone Carlos Gregorio, respecto al origen del derecho a la protección de datos personales en Ecuador, añadimos que la Constitución de 1998 señalaba: "El derecho a guardar reserva sobre sus convicciones políticas y religiosas. Nadie podrá ser obligado a declarar sobre ellas. En ningún caso se podrá utilizar la información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica" –art. 23.21–.

[11] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 17.

de datos como una libertad informática autónoma, derivada de la necesidad de incorporar derechos innovadores contenidos en instrumentos internacionales[12].

En el contexto latinoamericano se destacan la influencia de instrumentos internacionales como: las Directrices para la regulación de los archivos de datos personales informatizados de las Naciones Unidas; el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC); las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales; el Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo Adicional, también llamado Convenio 108+; y por supuesto, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[13]. Lógicamente, sobre la base de estos instrumentos, la adaptación de las legislaciones latinoamericanas al contexto internacional responde a "la preocupación por la necesidad de incrementar los intercambios comerciales transatlánticos, algo especialmente importante en un contexto de crisis económica"[14].

En el marco de la Unión Europea, la consolidación del derecho fundamental a la protección de datos personales también tuvo sus primeras manifestaciones, a través de la protección del derecho a la intimidad. Así, recordemos que "sólo se reconocían y protegían en el ámbito constitucional manifestaciones concretas de la intimidad, tales como el derecho a la inviolabilidad de domicilio y de las

[12] Estos instrumentos "son de diverso tipo y alcance, en la mayoría de los casos están presentados como guías o principios sugeridos o propuestos. Cabe resaltar asimismo que estos instrumentos buscan armonizar y ponderar el impacto de uno o varios de los derechos mencionados con otros intereses, vinculados a su propia esfera de acción". Cfr. Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", *Revista Transparencia y Sociedad – Consejo para la Transparencia de Chile*, Nro. 5 (2017):18.

[13] Precisamente, estos instrumentos constituyeron la base para la formulación de la Guía Legislativa de la OEA en 2015 y Estándares de protección de datos personales para los Estados Iberoamericanos en 2017.

[14] Troncoso, "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional".

comunicaciones, así como el secreto a la correspondencia"[15]. A lo que debe agregarse que fue el Tribunal Constitucional de Alemania el que basándose en el derecho a la dignidad y el derecho al libre desarrollo de la personalidad "garantizó la continuidad de las garantías básicas, consagradas con anterioridad, con la formulación de un nuevo derecho, el derecho a la autodeterminación informativa"[16].

Las causas para el desarrollo y adaptación del derecho fundamental a la protección de datos, en la era digital, en la Unión Europea se originan también a partir del fenómeno tecnológico y de los procesos económicos y comerciales.

Sobre este aspecto, apuntamos que:

> Si bien tanto la Directiva 95/46 CE como el Convenio 108 del Consejo de Europa reconocen principalmente principios y derechos y son tecnológicamente neutrales –y, por tanto, suficientemente flexibles–, han nacido a comienzos de los años ochenta y noventa del siglo pasado por lo que no han podido contener una referencia más expresa a los nuevos tratamientos de datos personales derivados de la revolución que se ha producido en las tecnologías de la información y de las comunicaciones. Esto obliga a repensar y a reforzar la normativa europea de protección de datos personales para que contemple y regule estas nuevas realidades que, si bien aportan principalmente oportunidades y ventajas, también conllevan la aparición de nuevos riesgos. Son tales los riesgos y las amenazas que ha llegado a afirmarse que debemos resignarnos a no tener privacidad –*you already have zero privacy. Get over it*– o si tenemos privacidad es porque alguien tolera que la tengamos[17].

En lo que respecta a su desarrollo, a partir de los procesos de integración, advertimos que "al par de conceptos intimidad-informática, se añade ahora uno más: el valor económico de los datos personales en relación con el respeto a los Derechos y en particular al Derecho a la intimidad"[18]. Por ello, en procesos de integración comercial-internacional, se evidencia "la necesidad de establecer marcos normativos de protección de la privacidad que permitan el flujo de datos y la interoperabilidad sin discriminación"[19].

Desde esta perspectiva, este capítulo está orientado a recorrer el reconocimiento constitucional del derecho a la protección de datos personales en el sistema jurídico

---

[15] Aristeo García González, La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado, *Boletín Mexicano de Derecho Comparado*, Nro. 120 (2007): pp. 743-778.
[16] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 89.
[17] Troncoso, "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional".
[18] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 92.
[19] Troncoso, "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional".

latinoamericano, con particular énfasis en aquellos países que han recibido reconocimiento internacional. Finalmente, se abordará de manera general, el proceso de reconocimiento de este derecho en el contexto de la Unión Europea, con especial referencia al modelo de regulación en España.

## 2. Reconocimiento del derecho fundamental a la protección de datos personales en Latinoamérica. Hacia un modelo de integración regional según la Guía Legislativa para los estados miembros de la OEA

La constitucionalización de los derechos no ha sido una tarea fácil dentro de los sistemas jurídicos. Su reconocimiento conlleva una serie de procesos de integración y discusión en el marco social, económico y jurídico. En el caso del derecho fundamental a la protección de datos, su origen se enmarca, a partir del debate que consideraba el derecho a la intimidad como insuficiente para proteger de manera integral a la persona, frente a los avances tecnológicos. Así, asumimos que esta libertad informática "representa la nueva libertad constitucional de la sociedad tecnológica como demuestran algunas experiencias de constituciones recientes y como puede recabarse, sin duda, a través de una interpretación evolutiva de las constituciones menos recientes"[20].

La consolidación de la protección de datos como un derecho fundamental ha recorrido, desde la necesidad de proteger el tratamiento de la información, frente a los avances tecnológicos y la obligación de ajustar los ordenamientos jurídicos a los procesos de integración comercial, hasta su reconocimiento constitucional como un derecho autónomo que, en lo público y privado, atribuya al titular de los datos el derecho a ejercer facultades de control sobre su propia información. Sobre esta base, "diversos organismos o instancias internacionales, tanto con vocación global como regional, y tanto de representación gubernamental, como también de

[20] Frosini, "Nuevas tecnologías y constitucionalismo", 32.

representación técnica e inclusive de sociedad civil han comenzado a elaborar lineamientos y principios"[21], los cuales se orientan a concretar un equilibrio global y regional. Por ello, a más de los instrumentos internacionales que hemos anotados, debe reconocerse, además, la importancia de la actividad desarrollada por la Organización de los Estados Americanos, en adelante OEA[22].

Una de las primeras propuestas de la OEA constituye el "Anteproyecto de Convención Americana sobre Autodeterminación Informativa" en 1997. Con fundamento en la Convención Americana sobre Derechos Humanos[23] –también llamada "Pacto de San José de Costa Rica"–; este anteproyecto se formuló con el objeto de concretar el respeto del derecho a la autodeterminación informativa "con relación a su vida privada y demás derechos de la personalidad; asimismo, la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes"[24]. Precisamente, el sistema jurídico latinoamericano se encuentra matizado por este esquema de protección. En todo caso, existen algunos países que han adoptado el modelo de regulación europeo; y también las recomendaciones formuladas por la OEA contenidas en la denominada Guía Legislativa de 2015[25].

Sobre el origen de este último instrumento, conviene señalar que, en 2012, el Comité Jurídico Interamericano (CJI) de la OEA presentó la "Propuesta de

[21] Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", 18.

[22] La Organización de los Estados Americanos (OEA) se considera como el organismo regional más antiguo del mundo. Tiene su origen en la Primera Conferencia Internacional Americana (Washington, 1889-1890).

[23] La Convención Americana sobre Derechos Humanos fue suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos el 22 de noviembre de1969, en San José de Costa Rica.

[24] Sobre el "Anteproyecto de Convención Americana sobre Autodeterminación Informativa", Véase la valoración de la propuesta realizada por el Comité Jurídico Interamericano en el Informe Anual de 1998, Disponible en: http://www.oas.org/es/sla/cji/docs/INFOANUAL.CJI.1998.ESP.pdf. Así también véase el texto completo del Anteproyecto, Disponible en: http://akane.udenar.edu.co/derechopublico/DATOS_AMERICA.pdf

[25] Los principios que señala la Guía Legislativa de la OEA tienen por objeto "proporcionar una guía para la preparación e implementación de Leyes nacionales y normas conexas en los Estados Miembros de la OEA. Cada Estado Miembro de la OEA debe adoptar e implementar una política clara y eficaz de apertura y transparencia para todos los adelantos, prácticas y políticas con respecto a los datos personales". Véase, Guía Legislativa para los estados miembros de la OEA (Principios de Privacidad y Protección de Datos Personales en las Américas): Recuperado de: http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

declaración de principios de Privacidad y Protección de Datos Personales en las Américas", la cual se formuló con el objeto de asegurar la protección de las personas, en virtud de los daños que podrían derivarse del tratamiento impropio de la información de carácter personal[26]. Para el siguiente año, esto es en 2013, la Asamblea General de la OEA en su cuadragésimo tercer período ordinario de sesiones encargó al CIJ la presentación de métodos, para la regulación y protección de los datos personales, considerando la inclusión de un proyecto de Ley Modelo[27].

Previo al cumplimiento de la Resolución AG/RES. 2811 (XLIII-O/13) de la Asamblea General de OEA, en el año 2014, el CJI propuso que era necesario realizar un estudio pormenorizado de los principios aprobados en 2012, tomando como referencia las normas internacionales que se hayan desarrollado para la regulación del derecho fundamental a la protección de datos[28]. Asimismo, para facilitar la elaboración de leyes nacionales, se sugirió la necesidad de una propuesta de Guía Legislativa que asegurara mayor interacción y debate de los principios de 2012. Un resultado útil para este objetivo, entre otros, resultó ser la compilación de instrumentos jurídicos pertinentes, relativos al espacio europeo. Entre ellos se destacan la Directiva General de la Unión Europea sobre la protección de datos y la

[26] En el 80 período ordinario de sesiones del Comité Jurídico Interamericano, la propuesta fue aprobada por unanimidad, mediante la Resolución CJI/RES. 186 (LXXX-O/12), en sesión celebrada el 9 de marzo de 2012. Los doce principios adoptados por el Comité Jurídico Interamericano, en su orden, son: Propósitos legítimos y justos; Claridad y consentimiento; Pertinencia y necesidad; Uso limitado y retención; Deber de confidencialidad; Protección y seguridad; Fidelidad de la información; Acceso y corrección; Información sensible; Responsabilidad; Flujo transfronterizo de la información y responsabilidad; y publicidad de las excepciones.

[27] La Asamblea General de la OEA, mediante la Resolución AG/RES. 2811 (XLIII-O/13) encargó al Comité Jurídico Interamericano la formulación de propuestas a la Comisión de Asuntos Jurídicos y Políticos, respecto a las distintas formas de regular la protección de datos personales, incluyendo un proyecto de Ley modelo sobre protección de datos. La idea, en este orden, suponía tomar en cuenta los estándares internacionales que se habían establecido en la Unión Europea.

[28] En el 84 período ordinario de sesiones del Comité Jurídico Interamericano se presentó la versión ampliada de los principios formulados en 2012, para la aceptación y aplicación de los Estados Miembros. Como antecedente, en el 83 período ordinario de sesiones del Comité, el Presidente solicitó al Doctor David P. Stewart para que actuara como relator del tema. Previo a la discusión de estos principios, en las sesiones de marzo de 2014, David P. Stewart –relator del tema– formuló sendas consultas a expertos internacionales en el ámbito de la Unión Europea, y a otros grupos regionales como la Red Iberoamericana de Protección de Datos Personales (RIPD).

Resolución de Estándares Internacionales de Madrid, más conocida como Resolución de Madrid[29].

Finalmente, en 2015 el CJI adoptó el informe formulado por David P. Stewart sobre los "Principios para la Privacidad y la protección de Datos Personales", los cuales consistieron, básicamente, en la precisión y fundamentación de los principios aprobados en 2012, y que, en definitiva, se traducen en la denominada Guía Legislativa de la OEA sobre la privacidad y la protección de datos personales [30]. Su finalidad se enmarcaría en guiar a los Estados Miembros en la formulación de leyes nacionales y normas relativas a la protección de datos personales[31].

Por otra parte, un organismo preocupado por desarrollar principios que se derivan de instrumentos internacionales es la Corte Interamericana de Derechos Humanos (CIDH). La CIDH se presenta como una instancia internacional de promoción y protección de los derechos. Y, además, se le reconoce su competencia para la interpretación y aplicación de las disposiciones de los principales instrumentos

[29] La Resolución de Madrid "recoge unas disposiciones generales, unos principios de protección de datos básicos, unos derechos de protección de los interesados y unas obligaciones de cumplimiento y supervisión (…) Es, por tanto, un documento nacido del diálogo y de la búsqueda del consenso que trata de integrar las sensibilidades de los distintos continentes, recogiendo los principios que son comunes a todos los modelos". Cfr. Antonio Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, (Valencia: Tirant lo Blanch, 2010), 246.

[30] En el 86 período ordinario de sesiones del Comité Jurídico Interamericano, en sesiones celebradas en marzo de 2015, se adoptó por consenso la denominada Guía Legislativa para los Estados Miembros, la cual se fundamenta en los doce principios aprobados en 2012. No obstante, en esta última versión, se introdujeron cambios en los principios siete, nueve y once; lo más significativo fue la sustitución del término "información" por el de "datos".

[31] La Guía Legislativa de la OEA, al respecto precisar que: "Cada Estado Miembro debe determinar cuál es la mejor manera de implementar estos principios en su ordenamiento jurídico interno. Sea por medio de Leyes, normas u otros mecanismos". En todo caso, conviene señalar que, en paralelo a esta Resolución, el Departamento de Derecho Internacional (DDI) de la OEA presentó una compilación de documentos básicos para el proceso de elaboración de una "Ley Modelo Interamericana sobre protección de datos personales". La compilación presentada por el DDI se compone de cinco apartados: a) Glosario Iberoamericano de Protección de Datos Personales; b) Estudio comparativo de la legislación en materia de protección de datos personales en Latinoamérica; c) Sistemas de Protección de Datos Personales (APEC y Unión Europea); d) Resoluciones, declaraciones, acuerdos y directrices internacionales; y e) Aportes del Centro de Protección de Datos Personales (CPDP) de la Ciudad Autónoma de Buenos Aires - Argentina y una Opinión Técnica del Instituto Federal de Acceso a la información y Protección de Datos (IFAI) de México.

interamericanos sobre derechos humanos[32]. En este marco, los precedentes jurisprudenciales, que la CIDH ha dictado en aspectos vinculados al tratamiento de la información personal, han sido progresivos y conexos a la vida privada. Por ejemplo, sobre el alcance de la protección a la vida privada refiere:

> El artículo 11.2 de la Convención protege la vida privada y el domicilio de injerencias arbitrarias o abusivas. Dicho artículo reconoce que existe un ámbito personal que debe estar a salvo de intromisiones por parte de extraños y que el honor personal y familiar, así como el domicilio, deben estar protegidos ante tales interferencias. La Corte considera que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública[33].

Así también, en relación a bienes jurídicos que se protegen, a través del derecho fundamental a la protección de datos personales, la CIDH sostiene que "la vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás"[34] –Caso Atala Riffo y niñas Vs. Chile; Sentencia de 24 de febrero de 2012; Serie C Nro. 239; párr. 162–; y que, en la relación a la tutela de la dignidad humana, se garantiza la protección de "la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales"[35] –Caso Artavia Murillo y otros Vs. Costa Rica; Sentencia de 28 de noviembre de 2012; Serie C Nro. 257; párr. 143–. En todo caso, las discusiones de la CIDH sobre el derecho a la dignidad humana, autonomía y libre desarrollo de la personalidad expresan, en nuestra opinión, la necesidad de

[32] Sobre la base de lo dispuesto en la Convención Americana de Derechos Humanos, la CIDH es competente para conocer de los asuntos relacionados con el cumplimiento de los compromisos contraídos por los Estados Partes en la Convención. Es decir: "Los Estados Partes en esta Convención se comprometen a respetar los derechos y libertades reconocidos en ella y a garantizar su libre y pleno ejercicio a toda persona que esté sujeta a su jurisdicción, sin discriminación alguna" –art. 1–.

[33] Cfr. Caso de las Masacres de Ituango Vs. Colombia, Sentencia de 1 de julio de 2006. Serie C Nro. 148. párr. 193 y 194.

[34] Sobre esta importante consideración, la CIDH –citando al Tribunal Europeo de Derechos Humanos– señala que "el derecho a la vida privada abarca la identidad física y social, el desarrollo personal y la autonomía personal de una persona". Cfr. párr. 135, *supra* nota 158, Caso Pretty Vs. Reino Unido (Nro. 2346/2), Sentencia de 29 de abril de 2002.

[35] Así también la CIDH –citando al Tribunal Europeo de Derechos Humanos– señala que "la efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona". Cfr. párr. 143, *supra* nota 228, Caso R.R. Vs. Polonia, (Nro. 27617/04), Sentencia del 26 de mayo de 2011.

contar con un reconocimiento más específico, en relación al derecho a la protección de datos personales.

A partir de estos ejemplos, evidenciamos dificultad para integrar en las resoluciones de la CIDH el reconocimiento de este derecho fundamental. Lo más próximo a la tutela de este derecho se recoge en las Sentencias: Caso González y otras Vs. México, relacionada con el manejo de bases de datos sobre personas desaparecidas, en la cual se dispuso que el Estado mexicano "en todo momento deberá proteger los datos personales contenidos en dichas bases de datos" –Serie C Nro. 205, párr. 512–. Así también en el Caso Gelman Vs. Uruguay, relacionado con el derecho a la identidad, por el cual se conceptualizó a este derecho como "el conjunto de atributos y características que permiten la individualización de la persona en sociedad"[36] –Serie C Nro. 221; párr. 122–.

Nos parecen interesantes los antecedentes fijados, tanto en las sesiones del Comité Jurídico Interamericano como en la propuesta del Departamento de Derecho Internacional y la jurisprudencia de la CIDH. Al respecto, son tres los antecedentes transcendentales. Primero, la propuesta de una Guía Legislativa fundamentada en varios principios estandarizados en el ámbito internacional para la protección de la información personal; segundo, abrir la posibilidad de generar una integración regional homogénea, en relación a la regulación de este derecho fundamental; y tercero, la dificultad de considerar el derecho a la protección de datos personales como un derecho autónomo, respecto al derecho a la intimidad[37].

[36] Es preciso anotar que la Guía Legislativa de la OEA define que un dato personal "abarca la información que identifica o puede usarse de manera razonable para identificar a una persona en particular de forma directa o indirecta". Es así que, la identidad personal se asocia con el derecho a la protección de datos personales, a partir, de los riesgos que supone el tratamiento de la información, frente al libre desarrollo de la personalidad.

[37] En este aspecto, reiteramos que "si bien ya existe una larga tradición que ampara el derecho a la vida privada, la protección de datos personales carece aún de una construcción propia, tanto normativa como jurisprudencial, a pesar de los incipientes esfuerzos y avances de la Organización de Estados Americanos (OEA) y de la Red Iberoamericana de Protección de Datos (RIDP). Cfr. María Maqueo Ramírez, Jimena Moreno y Miguel Recio Gayo, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", *Revista de Derecho (Valdivia)*, Nro. 1 (2017), 77-96. En todo caso, tras la emergencia sanitaria ocasionada por la pandemia del COVID-19, la Comisión Interamericana de Derechos Humanos ha reconocido la

Desde esta perspectiva, es preciso realizar una exégesis del reconocimiento constitucional del derecho fundamental a la protección de datos personales en Latinoamérica, considerando la evolución de su regulación, desde el derecho a la intimidad y del *habeas data,* hasta su configuración como un derecho de carácter fundamental y autónomo. En algunos casos, se observará el desarrollo de este derecho en normas sectoriales específicas. Así también se citarán precedentes jurisprudenciales y se revisará la previsión sobre la autoridad de control, que corresponde para la supervisión y regulación de este derecho.

## 2.1 El derecho fundamental a la protección de datos personales en Latinoamérica

Como ha señalado el CIJ, al parecer no existe uniformidad normativa en las Américas para regular el derecho a la protección de datos personales. Frente a las exigencias que plantea este derecho, es necesario "garantizar un nivel uniforme y elevado de protección para las personas físicas y eliminar los obstáculos a la circulación de datos personales"[38]. Tomando como referencia el caso europeo, precisamente, una de las virtudes ha sido universalizar principios y criterios jurídicos de protección, mediante Directivas y Reglamentos orientados a establecer, en cada país, un marco adecuado de regulación. Por ello, a falta de normativa común en el ámbito regional, es necesario analizar el régimen jurídico de protección que se ha desarrollado en Latinoamérica, por medio de un estudio comparado. En esta parte,

necesidad de preservar el derecho a la protección de datos personales, señalando que debe garantizarse "el derecho a la privacidad y los datos personales de la población, especialmente de la información personal sensible de los pacientes y personas sometidas a exámenes durante la pandemia. Los Estados, prestadores de salud, empresas y otros actores económicos involucrados en los esfuerzos de contención y tratamiento de la pandemia, deberán obtener el consentimiento al recabar y compartir datos sensibles de tales personas". Véase Resolución 1 /2020 sobre Pandemia y Derechos Humanos. Así también ha resaltado la importancia del respeto "de la privacidad y la protección de datos personales de las personas con COVID-19, así como la proliferación de herramientas digitales y aplicaciones que utilizan datos personales de la población, especialmente de información personal sensible en el contexto de la pandemia. Teniendo en cuenta la importancia de un marco jurídico robusto sobre protección de datos y el rol que juegan los órganos garantes en el cumplimiento de estos derechos". Véase Resolución 4 /2020 sobre Derechos Humanos de las personas con COVID-19.

[38] Milanes, "Desafíos en el debate de la protección de datos para Latinoamérica", 20.

el objetivo principal será identificar los principios constitucionales, leyes sectoriales, criterios jurisprudenciales y organismos que se han instituido para la regulación del derecho a la protección de datos.

Entendiendo que, "el nivel de protección de los derechos y libertades de las personas físicas referidas al tratamiento de dichos datos debe ser equivalente, mediante normativa coherente y homogénea"[39]. Estas características favorecen en el contexto internacional a garantizar la seguridad jurídica y confianza ciudadana, respecto al tratamiento de la información de carácter personal, en una sociedad en la que predomina el desarrollo tecnológico y la economía digital. Por estas razones, es de utilidad confrontar las adecuaciones normativas de cada país con los principios jurídicos sugeridos, fundamentalmente, por la Unión Europea y la OEA con el objeto de plantear un marco de protección integral que asegure suficientes garantías en el tratamiento de información personal. Como apreciaremos, el estudio comparado nos permitirá comprender la importancia de que el derecho a la protección de datos resguarda a la persona "–en el fondo, a la dignidad de la persona– frente a los tratamientos de datos personales porque estos tratamientos son vistos como un riesgo evidente para los derechos y libertades fundamentales de las personas que viene derivado del progreso tecnológico"[40].

### **2.1.1** Guatemala

Según Puccinelli, el primer país americano en contemplar a la protección de datos en el ámbito constitucional fue Guatemala en la Constitución de 1985[41]. Esta

[39] Ibíd.

[40] Antonio Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada*, Nro. 49 (2018), 187-266.

[41] Cfr. Oscar Puccinelli, "Tipos y subtipos de *habeas data* en América latina", Recuperado de: Base de datos: Vlex.com.ec: https://app.vlex.com/#/vid/26542396. Hay que señalar que la Constitución de 1985 refería que: "Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos" –art. 31–.

Constitución –reformada en 1993 por el Congreso de la República y aprobada en su reforma mediante referéndum en ese mismo año– garantiza la protección de datos personales, a través del reconocimiento de los derechos de acceso, corrección, rectificación y actualización de la información –art. 31–.

A pesar de no contemplar a la protección de datos como un derecho autónomo, su tutela, además, puede invocarse en la protección constitucional que garantiza que "todos los seres humanos son libres e iguales en dignidad y derechos –art. 4–; y también en el reconocimiento de que "los derechos y garantías que otorga la Constitución no excluyen otros que, aunque no figuren expresamente en ella, son inherentes a la persona humana" –art. 44–. Precisamente, a partir del respeto de la dignidad humana; un derecho que es inherente a las personas es el derecho a la protección de datos personales. En este sentido, insistimos en que "esta relación del derecho a la protección de datos con el resto de derechos fundamentales fortalece su vinculación con la dignidad de la persona"[42].

A partir del Decreto Nro. 57-2008 de octubre de 2008, el tratamiento de los datos personales presenta una regulación sectorial, mediante la promulgación de la Ley de Acceso a la Información Pública. Así, la protección de datos personales surge, paralelamente, a la necesidad de regular el derecho de acceso a la información pública y se afianza en las potestades asignadas en la garantía del *habeas data*[43].

En este país, no existen disposiciones regulatorias, sobre una autoridad administrativa de supervisión y control del derecho a la protección de datos personales. En todo caso, en la Ley de Acceso a la Información Pública se hace referencia a la Procuraduría de los Derechos Humanos como la autoridad

[42] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 75.

[43] La Ley de Acceso a la Información Pública refiere al *habeas data* como "la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización. Los datos impersonales no identificables, como aquellos de carácter demográfico recolectados para mantener estadísticas, no se sujetan al régimen de *habeas data* o protección de datos personales de la presente Ley" –art. 9.4–. Es importante señalar que el 20 de agosto del 2009 se presentó una iniciativa de Ley de Protección de Datos Personales, la cual aún no tiene el respaldo en el Congreso de la República de Guatemala.

reguladora para promover el buen funcionamiento institucional, así como recibir acciones o recursos que vayan en contra de los derechos humanos[44]. Este organismo, en su informe anual, de 2015, advertía que "el PDH ha recibido 358 denuncias por la supuesta violación a la intimidad por comercialización de datos personales. Estas denuncias indican que diferentes entidades publican en sus portales electrónicos datos personales sin el consentimiento de la persona involucrada"[45]. Según el informe citado, se estimó que esta problemática se ha ido acrecentando, a pesar de la normativa existente en la Ley de Acceso a la Información Pública y de la jurisprudencia de la Corte de Constitucionalidad de Guatemala[46].

En lo que corresponde a los precedentes jurisprudenciales, un enfoque preliminar sobre la protección de datos personales está contenido en la Resolución de la Corte en el expediente 863-2011, el cual señala:

> Del derecho al reconocimiento de la dignidad humana, implícitamente garantizado, entre otros, en los primeros cinco artículos de la Constitución Política de la República, dimanan, por el contenido esencial de este derecho, aquellos relacionados a la intimidad, al honor y a la privacidad, los cuales, en su conjunto, también garantizan la existencia y goce de otro derecho: el referido a la autodeterminación informativa.

Por tanto, acreditaríamos el reconocimiento que se hace sobre el derecho a la protección de datos, a partir del derecho a la dignidad humana; y así también su conceptualización como un derecho autónomo, caracterizado por ser un instituto de

---

[44] El art. 47 de la Ley de Acceso a la Información Pública, al determinar las facultades de la Procuraduría de los Derechos Humanos vincula las atribuciones de ésta, conforme con lo dispuesto en los arts. 13, 14 y, demás, aplicables en la Ley de la Comisión de los Derechos Humanos del Congreso de la República y del Procurador de los Derechos Humanos, Decreto Número 54-86 del Congreso de la República.

[45] Procuraduría de los Derechos Humanos de Guatemala, Informe Anual Circunstanciado: Situación de los Derechos Humanos y Memoria de Labores 2015, p. 380. Disponible de: https://www.pdh.org.gt/biblioteca-digital-informes-informes-anuales/

[46] Por ejemplo, la Ley Nro. 57-2008 (Ley de Acceso a la Información Pública), sobre la comercialización de datos personales señala que: "Quien comercialice o distribuya por cualquier medio, archivos de información de datos personales, datos sensibles o personales sensibles, protegidos por la presente Ley sin contar con la autorización expresa por escrito del titular de los mismos y que no provengan de registros públicos, será sancionado con prisión de cinco a ocho años y multa de cincuenta mil a cien mil Quetzales y el comiso de los objetos instrumentos del delito. La sanción penal se aplicará sin perjuicio de las responsabilidades civiles correspondientes y los daños y perjuicios que se pudieran generar por la comercialización o distribución de datos personales, datos sensibles o personales sensibles" –art. 64–.

garantía de otros derechos fundamentales, como la intimidad y privacidad de las personas. En este punto, dicha Resolución precisa que:

> Los avances de la tecnología informática generan a su vez una dificultad en cuanto a proteger adecuadamente el derecho a la intimidad y a la privacidad de una persona individual. Una solución a esa problemática ha sido la de reconocer el derecho a la autodeterminación informativa del individuo, cuyo goce posibilita a éste un derecho de control sobre todos aquellos datos referidos a su persona y, a su vez, le garantiza la tutela debida ante un uso indebido (es decir, sin su autorización) y con fines de lucro, por parte de un tercero, de todos aquellos datos personales susceptibles de tratamiento automatizado, con los cuales se integra una información identificable de una persona

Asimismo, la Corte en el expediente 3552-2014, sobre la comercialización de datos personales ha señalado que:

> El derecho a la autodeterminación informativa es positivo a favor de la población en general, al ser reconocido en los artículos 4º y 44 de la Constitución Política de la República de Guatemala, 12 de la Declaración Universal de Derechos Humanos, 11.2 de la Convención Americana sobre Derechos Humanos (…) La obtención de datos personales que puedan formar una base de datos, susceptible de transmisión vía medios de comunicación masiva o electrónica -por medio de la informática-, debería ser objeto de regulación por parte de una ley (…) En Guatemala no existe tal regulación, y en tanto no la haya, para no incurrir en situaciones *legibus solutus,* a criterio de esta Corte toda comercialización de información de datos de una persona debe estar sujeta a que esa información fuera proporcionada voluntariamente por la persona, cuyos datos serán objeto de comercialización.

De esta manera es como se encuentra garantizado el derecho fundamental a la protección de datos personales. Como un derecho, se caracteriza por tener un reconocimiento que nace del derecho a la dignidad humana y del derecho a la intimidad. En este marco, es importante destacar la actividad jurisdiccional que desarrolla la Procuraduría de los Derechos Humanos como una autoridad reguladora para la garantía de este derecho fundamental[47].

[47] Al respecto, según el Informe Anual de 2015, este organismo señala que: "Durante 2014, el PDH promovió una acción de amparo a favor de la población que había denunciado ser perjudicada por figurar en las bases de datos de entidades mercantiles que comercializan datos personales sin autorización del titular de la información. El amparo fue otorgado por el Juzgado Décimo de Primera Instancia Civil del departamento de Guatemala (…) Dicha sentencia fue apelada ante la Corte de Constitucionalidad (…) que fue declarada sin lugar en sentencia, expediente 3552-2014 (…) En dicha sentencia, la Corte de Constitucionalidad (CC) estableció que la plena eficacia del derecho a la autodeterminación informativa debe permitir a la persona: el derecho a la actualización de sus datos; el derecho a la rectificación por información errónea, incompleta o inexacta de sus datos; el derecho a la reserva de cierta información que sobre ella se obtenga, y que aun cuando esta pueda ser legalmente requerida, se mantenga en grado de confidencialidad para terceras personas ajenas a la situación que motivó el requerimiento; y el derecho a la exclusión, en circulación informativa abierta o restringida, de información que pueda considerarse sensible para el interesado". Cfr. Procuraduría de los Derechos Humanos de Guatemala, Informe Anual Circunstanciado: Situación de los Derechos Humanos y Memoria de Labores 2015, p. 380.

### **2.1.2** Nicaragua

La Constitución de 1987 protegía el derecho a la vida privada de las personas y la familia[48]. Así, la protección de datos personales podía entenderse, a partir del respeto a la vida privada. Si bien, esta Constitución no realizaba referencia alguna acerca del *habeas data*, hay que considerar que el recurso de amparo se instituía como una acción constitucional, encaminada a tutelar toda acción u omisión que vulnere los derechos constitucionales[49].

En 2014, mediante la Ley Nro. 854 reformatoria parcial a la Constitución, se reconoce la naturaleza del derecho a la protección de datos personales, a través del reconocimiento de los principios de deber de información y de finalidad en el tratamiento de la información personal[50]. Así, en su art. 7, el cual reformó el art. 26.3 de la Constitución introduce el derecho de las personas a "conocer toda información que sobre ella se haya registrado en las entidades de naturaleza privada y pública, así como el derecho de saber por qué y con qué finalidad se tiene esa información"[51]. Asimismo, por medio del art. 43, que reformó el art. 190 de la Constitución, la Ley Nro. 854 incluyó el recurso de *habeas data* como un mecanismo

[48] La Constitución de 1987 refería que: "Toda persona tiene derecho: 1) A su vida privada y a la de su familia. 2) A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones. 3) Al respeto de su honra y reputación (…) La Ley fija los casos y procedimientos para el examen de documentos privados, libros contables y sus anexos cuando sea indispensable para esclarecer asuntos sometidos al conocimiento de los tribunales de justicia o por motivos fiscales" –art. 26–.

[49] Respecto al recurso de amparo, la Constitución refiere que esta garantía se dirige en "contra de toda disposición, acto o resolución y en general en contra de toda acción u omisión de cualquier funcionario, autoridad o agente de los mismos que viole o trate de violar los derechos y garantías consagrados en la Constitución Política" –art.188–.

[50] La Ley Nro. 854 fue aprobada el 29 de enero de 2014; y publicada en la Gaceta Nro. 26 del 10 de febrero del mismo año.

[51] De esta manera, puede advertirse que del art. 26.3 de esta Constitución "se deriva la Ley 787, Ley de protección de datos personales, publicada en La Gaceta, Diario Oficial Nro. 61 del 29 de marzo de 2012 (LPDP) y su reglamento, Decreto 36-2012, Reglamento de la Ley Nro. 787, Ley de protección de datos personales, publicado en La Gaceta, Diario Oficial Nro. 200 del 19 de octubre de 2012 que tienen como objeto: la protección de la persona natural o jurídica, frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa". Cfr. Noelia Zeledón Arancibia, "La posible implementación de la portabilidad numérica en Nicaragua", *Revista de Derecho*, Nro. 18 (2015), ISSN 1993-4505, 18 – 55.

de control constitucional que –en lo público y privado–, tutelaría el derecho a la protección de datos[52]. Así, el texto reformado reconoció:

> 1) El Recurso de *Habeas data* como garantía de tutela de datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos, de naturaleza pública o privada, cuya publicidad constituya invasión a la privacidad personal y tenga relevancia con el tratamiento de datos sensibles de las personas en su ámbito íntimo y familiar. El Recurso de *Habeas data* procede a favor de toda persona para saber quién, cuándo, con qué fines y en qué circunstancias toma contacto con sus datos personales y su publicidad indebida.

A diferencia de la Constitución de 1987, la ampliación del derecho a la protección de datos personales es notable. Se reconocen los riegos sobre el tratamiento de la información en el ámbito público y privado. Asimismo, se consagra el *habeas data* como una garantía que tutela los datos personales.

Ahora bien, a esta reforma constitucional le antecede la Ley Nro. 787 de Protección de Datos Personales de 2012 cuyo objeto es la protección de las personas "frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa"[53]. Una novedosa regulación que introduce esta Ley es el derecho al olvido digital –art. 10–. Así, bajo esta garantía, "el titular de datos personales tiene derecho a solicitar a las redes sociales, navegadores y servidores que se supriman y cancelen los datos personales que se encuentren en sus ficheros"[54]. Considerando la evolución tecnológica y las problemáticas que se derivan del tratamiento de la información personal, el reconocimiento del derecho al olvido digital constituye un avance significativo en la legislación sobre protección de datos, a partir de los riesgos que presentan las redes sociales e Internet.

---

[52] El art. 190 de la Constitución de 1987 refería que "La Ley de Amparo regulará los recursos establecidos en este capítulo".

[53] La aprobación de esta Ley tiene como antecedente, según sus considerandos, la necesidad de equilibrar otros derechos, a partir, de la Ley Nro. 621 de Acceso a la Información Pública; e implementar las garantías necesarias para los derechos consagrados, en ese entonces, por la Constitución de 1987. Dicha Ley fue aprobada el 21 de marzo de 2012; y publicada en la Gaceta Nro. 61 del 29 de marzo de 2012.

[54] Morena Zavaleta, "El derecho al olvido digital en la Ley de Protección de Datos Personales de Nicaragua (Ley 787)", *Revista Latinoamericana de Protección de Datos Personales*, Nro. 2 (2014), ISSN 2422-6769.

Respecto a la autoridad de protección de datos personales, la Ley Nro. 787 dispuso la creación de la Dirección de Protección de los Datos Personales, adscrita al Ministerio de Hacienda y Crédito Público. Así, la naturaleza de esta autoridad se orienta al "control, supervisión y protección del tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada" –art. 28–. Ante la carente previsión normativa sobre las funciones administrativas que debería desarrollar esta Dirección, las resoluciones que se han expuesto sobre la materia proceden más bien desde la vía jurisdiccional[55].

La Sala de lo Constitucional de la Corte Suprema de Justicia, mediante Sentencia Nro. 19 de 2004, ha señalado que[56]:

> El derecho a la privacidad es un derecho personal, en el que las personas tienen el derecho de controlar la información que sea relevante en su vida privada, es un derecho que busca desarrollar un espacio propio, un lugar donde poder estar solos, sin intromisiones inoportunas. Es un espacio que le concierne sólo a esa persona y que queda reservado de los demás. Este espacio es la consecuencia de la individualidad y autonomía correspondientes a todo ser humano, porque toda persona tiene derecho a exigir que sus asuntos no sean expuestos o examinados por terceros, sin haber dado su consentimiento.

Según este criterio, la protección de la información personal se enmarca en la garantía del derecho a la privacidad. En este contexto, consideramos que la falta de desarrollo de criterios judiciales sobre el derecho a la protección de datos se debe: primero, a la relativa novedad de la promulgación de la Ley Nro. 787 sobre protección de datos y la reforma constitucional del *habeas data*; y segundo, a la falta de organización en la vía administrativa, respecto a las funciones de la Dirección de Protección de los Datos Personales[57].

---

[55] La Dirección de Protección de los Datos Personales debería ser un órgano administrativo adscrito al Ministerio de Hacienda y Crédito Público. No obstante, hasta la presente fecha no se ha podido confrontar ninguna información relativa a las funciones de esta Dirección. Este criterio se afianza en la búsqueda realizada en la página del Ministerio: http://www.hacienda.gob.ni/.

[56] De la investigación realizada, se anota como la Sentencia más actualizada en el portal de consultas de jurisprudencia del Poder Judicial de Nicaragua. http://www.poderjudicial.gob.ni/scons1/jurisprudencia.asp.

[57] En todo caso, señalamos que el control, la supervisión y la tutela de este derecho fundamental también recae en la administración, en general, por cuanto "este derecho a la inviolabilidad de la correspondencia y de la protección de datos personales se ve palpado en la responsabilidad de las operadoras de servicios de telecomunicaciones de ser garantes de la confidencialidad de la información a la que tienen acceso". Cfr. Noelia Zeledón Arancibia, "La posible implementación de la portabilidad numérica en Nicaragua".

### **2.1.3** Brasil

Desde 1988, la Constitución de Brasil consagra un modelo de protección de la información de carácter personal basado en la tutela del derecho a "la intimidad, la vida privada, el honor y la imagen de las personas" –art. 5.10–; y garantía del *habeas data* que asegura el conocimiento y rectificación "de la información relacionada con la persona, contenida en registros o bases de datos de entidades gubernamentales o de carácter público" –art. 5.72–[58].

El *habeas data* supuso la introducción de un nuevo recurso en el derecho constitucional orientado, específicamente, a la "tutela de la honra, de la tranquilidad, del patrimonio, de la vida privada, entre diversos valores, contra los atentados efectuados por organismos públicos o de carácter público, en la anotación de datos e informaciones acerca de las personas"[59]. Pese a considerarse como el primer país en introducir la acción de *habeas data* en 1988, el desarrollo de la protección de datos estaba contextualizado desde el derecho a la privacidad[60].

Como señala Danilo Doneda:

> La información personal es, casi por reflejo vinculado a la privacidad mediante una simple ecuación básica que asocia un mayor grado de privacidad a la menor de la información personal y viceversa. Esta ecuación al momento de la terminación de todos los complejos problemas que rodean a esta relación, puede servir como un punto de partida para ilustrar cómo la protección de la información personal vino a buscar refugio en nuestro sistema legal: como una rama de la protección del derecho a la privacidad[61].

Al no contemplarse en la Constitución a la protección de datos como un derecho fundamental autónomo, la protección de la información personal tuvo, inicialmente,

---

[58] Luiz Pinto Ferreira, "Os instrumentos processuais protetores dos direitos no Brasil", en Domingo García Belaunde (coord.), *La jurisdicción constitucional en Iberoamérica*, (Madrid, Dykinson, 1997), 421.

[59] Sobre estas disposiciones, además, la Constitución de 1988 refiere que: "Son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su violación" –art. 5.10–; y "Se concederá *´habeas data´*: a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo" –art. 5.72–.

[60] Cfr. Oscar Puccinelli, "Tipos y subtipos de *habeas data* en América latina".

[61] Danilo Doneda, "A proteção dos dados pessoais como direito fundamental, *Revista Espaço Jurídico*, Nro.2 (2011), 91-108.

un interesante desarrollo en la normativa sectorial. Se destacan la promulgación de la Ley Nro. 9296 orientada a proteger el derecho a la privacidad de las comunicaciones, a partir de cualquier tipo de interceptación telefónica[62]; la Ley Nro. 9507 de *Habeas Data* destinada a asegurar el conocimiento de las personas sobre el tratamiento de su información contenida en entidades gubernamentales o públicas[63]; y la Ley Nro. 12.965 que establece principios, garantías, derechos y deberes para el uso de Internet, enmarcados, entre otras garantías, en la protección de datos personales –art. 3.3–[64].

Conviene destacar que el órgano competente para tramitar el *habeas data* es el Supremo Tribunal Federal. Al respecto, se apunta que, "se intenta de tal modo excluir a jueces de primera o de segunda instancia el conocimiento de decisión de cuestiones de posible gran importancia, donde por lo común surgirán temas próximos a la seguridad nacional"[65]. Así, este Tribunal estableció algunos precedentes jurisprudenciales relacionados con el tratamiento de la información personal. Por ejemplo, sobre la privacidad e interceptación de comunicaciones personales, mediante la Resolución 103.236 señala que:

> La Ley 9.296 / 1996 no hizo más que establecer directrices para resolver los conflictos entre la privacidad y la obligación del Estado de hacer cumplir las leyes penales. A pesar del

[62] La Ley N ° 9296, de 24 de julio de 1996 menciona que: "Las disposiciones de la presente Ley se aplica a la interceptación del flujo de las comunicaciones de los sistemas de información y la telemática" –art 1–.

[63] La Ley N ° 9507, de 12 de noviembre de 1997, que regula el derecho de acceso a la información y el procedimiento judicial de *habeas data* refiere que el *habeas data* está dirigida: "I- para asegurar el conocimiento de informaciones relativas a la persona del peticionario, contenida registro o base de datos de entidades gubernamentales o de las entidades públicas; II- para la corrección de los datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo; III- a la nota en las localidades en cuestión de disputas o explicación que se da cierto, pero justificable y está bajo judicial o amistosa pendiente" –art. 7–.

[64] Así por ejemplo, en el marco de garantía para el acceso a Internet, se garantiza a los usuarios el derecho a "no suministrar a terceros de sus datos personales, incluyendo registros de conexión, y de acceso a aplicaciones de Internet, salvo mediante consentimiento libre, expreso e informado o en las hipótesis previstas por Ley" –art. 7.7–; y así también el derecho a "informaciones claras y completas sobre recolección, uso, almacenamiento, tratamiento y protección de sus datos personales, que sólo podrán ser utilizados para fines que: a) justifiquen su recolección; b) no estén vedadas por la legislación; y c) estén especificadas en los contratos de prestación de servicios o en términos de uso de aplicaciones de Internet" –art. 7.8–.

[65] Néstor Pedro Sagués, "El *Habeas Data*: su desarrollo constitucional", en *V Congreso Iberoamericano de derecho Constitucional*, (México, Instituto de Investigaciones Jurídicas, 1998), 859-872.

> carácter excepcional de la medida, el artículo XII posibilita, expresamente, una vez cumplidos los requisitos constitucionales, la interceptación de las comunicaciones telefónicas. Y tal permiso existe, por el simple hecho de que los derechos y garantías constitucionales no pueden servir de manto protector a prácticas ilícitas[66].

En lo que se refiere al tratamiento de la información financiera, la Resolución 84.758 señala que:

> La violación de la confidencialidad no puede ser manipulada, de manera arbitraria, por el Poder Público o sus agentes. Es que, si no fuera así, la violación del secreto se convertiría, ilegítimamente, en instrumento de búsqueda generalizada y de injustificable indiscriminación a la esfera de la intimidad de las personas, lo que resultaría al Estado, en disconformidad con los postulados que gobiernan un régimen democrático, o poder absoluto de resquebrajar, sin ninguna limitación, registros confidenciales[67].

Asimismo, la Resolución 673707 acerca del *habeas data* señala:

> 4. El carácter público de todo registro o base de datos que contiene información que sea o puedan ser transmitidas a terceros y que no sea de uso privativo de un organismo o entidad productora o depositaria de información es inequívoco. (art. 1º, Lei nº 9.507/97). 5. El registro de datos ser entendido en su sentido más amplio, abarcando todo lo que siga respecto al interesado, sea de modo directo o indirecto (…) 6. En *legitimatio ad causam* para interpretación el *Habeas data* extiéndase a personas físicas y jurídicas, nacionales y extranjeras, por cuanto es garantía constitucional de los derechos individuales y colectivos. 7. Los contribuyentes fueron asegurados constitucionalmente en el derecho a conocer las informaciones en relación con su objeto en bancos de datos públicos o de carácter público, en razón de la necesidad de preservar el estado de su nombre, planificación empresarial, estrategia de inversión y, en especial, la recuperación de los impuestos pagados indebidamente, verbis: Art. 5º. …LXXII. Considérese *habeas data* para asegurar el conocimiento de informaciones relativas a la persona del peticionario, constantes en registros o bases de datos de entidades gubernamentales o de carácter público, considerado como un recurso, una garantía, un remedio constitucional a disposición de los ciudadanos para que puedan ejercitar derechos subjetivos que están siendo impedidos[68].

---

[66] Cfr. a continuación el texto original de la Resolución: “A Lei 9.296/1996 nada mais fez do que estabelecer as diretrizes para a resolução de conflitos entre a privacidade e o dever do Estado de aplicar as leis criminais. Em que pese ao caráter excepcional da medida, o inciso XII possibilita, expressamente, uma vez preenchidos os requisitos constitucionais, a interceptação das comunicações telefônicas. E tal permissão existe, pelo simples fato de que os direitos e garantias constitucionais não podem servir de manto protetor a práticas ilícitas”.

[67] Cfr. a continuación el texto original de la Resolución: "A quebra de sigilo não pode ser manipulada, de modo arbitrário, pelo Poder Público ou por seus agentes. É que, se assim não fosse, a quebra de sigilo converter-se-ia, ilegitimamente, em instrumento de busca generalizada e de devassa indiscriminada da esfera de intimidade das pessoas, o que daria ao Estado, em desconformidade com os postulados que informam o regime democrático, o poder absoluto de vasculhar, sem quaisquer limitações, registros sigilosos alheios”.

[68] Cfr. a continuación el texto original de la Resolución: “4. O caráter público de todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações é inequívoco (art. 1º, Lei nº 9.507/97). 5. O registro de dados deve ser entendido em seu sentido mais amplo, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto. (…) 6. A legitimatio ad causam para interpretação de *Habeas data* estendese às pessoas físicas e jurídicas,

Hasta aquí, el orden normativo sectorial y la jurisprudencia contextualizó a la protección de los datos, a través del derecho a la intimidad en el ámbito de las comunicaciones de carácter personal. Se introdujo un conjunto de garantías, derechos y deberes para el uso de Internet. Naturalmente, el *habeas data* significa en el ordenamiento constitucional brasileño la más alta expresión garantista del derecho fundamental a la protección de datos.

A pesar de que este derecho no cuenta con un reconocimiento autónomo en la Constitución, el dato positivo es que –a partir de los riesgos que representan las tecnologías, frente al tratamiento automatizado de la información– la protección de la personalidad se ampara en las garantías constitucionales de igualdad, libertad y dignidad de la persona humana en conjunto con la protección de la intimidad y vida privada[69]. Tomando en consideración que el amparo de la información personal queda bajo la tutela de las garantías constitucionales que se mencionan, puntualizamos que la protección de datos en el ordenamiento jurídico brasileño "no se estructura a partir de un complejo normativo unitario. La Constitución Brasileña contempla el problema de la información inicialmente por medio de las garantías a la libertad de expresión y del derecho a la información"[70].

En todo caso, se espera que la reciente Ley Nro. 13.709 –Ley General de Protección de Datos, que entró en vigencia en agosto de 2020– sea el marco normativo idóneo que garantice que el derecho a la protección de datos cumpla con estándares internacionales, por cuanto esta Ley tiene como objetivo "no solo garantizar los derechos individuales, sino también fomentar el desarrollo económico, tecnológico y la innovación en el país, sobre la base de reglas precisas para el uso transparente,

---

nacionais e estrangeiras, porquanto garantia constitucional aos direitos individuais ou coletivas. 7. Aos contribuintes foi assegurado constitucionalmente o direito de conhecer as informações que lhes digam respeito em bancos de dados públicos ou de caráter público, em razão da necessidade de preservar o status de seu nome, planejamento empresarial, estratégia de investimento e, em especial, a recuperação de tributos pagos indevidamente, verbis: Art. 5º. …LXXII. Concederseá *habeas data* para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, considerado como um writ, uma garantia, um remédio constitucional à disposição dos cidadãos para que possam implementar direitos subjetivos que estão sendo obstaculados".

[69] Cfr. Danilo Doneda, "A proteção dos dados pessoais como direito fundamental, 103.

[70] Ibíd.

adecuado y legítimo de la información personal de las personas"[71]. En este sentido, destacamos que la Ley Nro. 13.709 tiene por objeto proteger los derechos fundamentales "de libertad y privacidad y el libre desarrollo de la personalidad de la persona física" –art. 1–; y asegurar la protección de datos personales, mediante el respeto a "la privacidad; autodeterminación informativa; libertad de expresión, información, comunicación y opinión; la inviolabilidad de la intimidad, el honor y la imagen; desarrollo e innovación económica y tecnológica; libre empresa, libre competencia y protección del consumidor; y los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por parte de las personas físicas" –art. 2–.

La nueva Ley brasileña constituye un importante modelo en el contexto latinoamericano. Supone un esquema de protección de la información de carácter personal, el cual se sustenta en el respeto de los derechos humanos y en la dignidad de las personas. "Influenciado directamente por las regulaciones europeas, el LGPD aparece en Brasil, garantizando principios y derechos para los interesados, además de hacer que las hipótesis de recolección y tratamiento sean positivas"[72]. De esta manera, este marco de protección de datos es, esencialmente, importante, por cuanto:

> En términos generales, la base para garantizar una protección adecuada que se materialice en el control que la persona pueda tener sobre el tratamiento de sus datos personales, se constituye mediante unos criterios de legitimación, los principios de la protección de datos, la posibilidad de ejercer derechos por parte del titular de los datos y la supervisión, misma que puede concretarse en la tutela de la persona a la que se refieren los datos personales que son objeto de tratamiento, así como la atribución y el ejercicio de potestades de investigación y sanción por parte de una autoridad de control independiente[73].

[71] Paulo Rodríguez, Thays Castaldi y Giovanna Bruno. "A Nova Lei Geral de Proteção de Dados no Brasil", *Revista Latinoamericana de Protección de Datos Personales*, Nro. 5 (2018). Disponible en: https://tinyurl.com/yxxq3bmv. Es conveniente señalar que, en 2016 se presentó ante la Cámara de Diputados el Proyecto de Ley 5.276/2016 que –además de modificar la Ley Nro. 12.965- disponía considerar al tratamiento de datos personales como una garantía de libre desarrollo de la personalidad y dignidad de las personas naturales. Puede consultarse el texto oficial del proyecto en el siguiente enlace: https://tinyurl.com/sv59ate.

[72] Ibíd.

[73] Maqueo Ramírez, Moreno y Recio Gayo, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", 92.

Ahora bien, en relación a la autoridad de protección de datos personales, la Medida Provisional Nro. 869, que complementa a la Ley Nro. 13.709, dispone la creación de la Autoridad Nacional de Protección de Datos. Así, a partir de dicha Medida Provisional, se garantiza la autonomía técnica de la ANPD y la constituye como "un órgano de la administración pública federal, miembro de la Presidencia de la República", que tiene como responsabilidad "garantizar, implementar y supervisar" el cumplimiento de la Ley Nro. 13.709[74]. En todo caso, mediante el Decreto Nro. 10.474, se reconoció que dicha autoridad es un órgano, "dotado de autonomía técnica y decisoria, con jurisdicción en el territorio nacional y con sede en el Distrito Federal" –art. 1–[75].

### **2.1.4** Colombia

La Constitución de 1991 garantiza el derecho a la protección de datos personales, a través de los derechos relacionados con la intimidad y el buen nombre; conocer, actualizar y rectificar la información recogida en entidades públicas y privadas; y el respeto de la libertad informática en la recolección, tratamiento y circulación de datos –art. 15–[76]. Sobre la base de la libertad informática y demás garantías reconocidas en la Constitución, "el constituyente definió la protección de la intimidad

[74] Antes de la vigencia de la Ley General de Protección de Datos, la Agencia Nacional de Telecomunicaciones podía considerarse como una autoridad de control en la materia. Precisamente, la Ley Nro. 9.472/97 reconoce que este organismo actúa como una autoridad de vigilancia y control de los bienes jurídicos que se desprenden del derecho de la privacidad en el sector de las telecomunicaciones. Así, para el ejercicio de su jurisdicción, amparada en los arts. 8 y 9 de esta Ley, la Agencia se considera como una autoridad independiente en el ámbito administrativo y jerárquico; y con autonomía financiera. Su actividad está orientada a reprender las violaciones de los derechos de los usuarios y actúa como una instancia de control, supervisión y sanción.

[75] El Decreto Nro. 10.474, además, señala que dicha autoridad "tiene el objetivo de proteger los derechos fundamentales de la libertad e intimidad y el libre desarrollo de la personalidad de la persona natural, guiados por lo dispuesto en la Ley Nro. 13.709, de 14 de agosto de 2018" –art. 1–.

[76] En este marco, la Constitución de 1991 refiere que: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución" –art. 15–.

de la persona, cuando ella es fuente de información personalísima y cuando esa información se encuentra en los llamados bancos de datos, públicos o privados"[77].

Inicialmente, según el art. 86 de la Constitución, la acción de tutela se constituyó como un mecanismo procesal para la protección de los derechos fundamentales reconocidos en la Constitución[78]. Lógicamente, también para la tutela de aquellos derechos relacionados con la protección de la información de carácter personal. No obstante, desarrollando el art. 15 de la Constitución, la Ley 1266 de 2008 sobre el "*Habeas data"* se orienta a tutelar los derechos, libertades y garantías relacionadas con la recolección, tratamiento y circulación de datos personales[79]. De este modo, la Ley 1266 se considera como una garantía que "refiere a la protección y respeto del derecho a la autodeterminación informativa que contiene la intimidad e idoneidad personal que surge de la información suministrada por ésta, según se deduce de lo consagrado en el artículo 15 de la Carta Política"[80].

Por otra parte, la Ley Estatutaria 1581 se constituye como una Ley General de protección de datos, por cuanto establece disposiciones generales y principios aplicables al tratamiento de la información personal[81]. Así, consideramos que dicha

---

[77] Luis Freddyur Tovar, "Positivación y Protección de los Derechos Humanos: Aproximación Colombiana", *Revista Criterio Jurídico de la Pontificia Universidad Javeriana*, Nro. 2 (2008), 45-72.

[78] En este caso, la Constitución de 1991 hace referencia que: "Toda persona tendrá acción de tutela para reclamar ante los jueces, en todo momento y lugar, mediante un procedimiento preferente y sumario, por sí misma o por quien actúe a su nombre, la protección inmediata de sus derechos constitucionales fundamentales, cuando quiera que éstos resulten vulnerados o amenazados por la acción o la omisión de cualquier autoridad pública" –art. 86–.

[79] La Ley 1266 de *Habeas data* señala que: "La presente Ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política" –art. 1–. En todo caso, esta disposición también prescribe que dicha Ley se orienta a desarrollar el derecho a la información establecido en el art. 20 de la Constitución, "particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países" –art. 1–. Así, advertimos que, "al analizar el contenido de la norma se observa que se encuentra orientada a la protección de los datos comerciales y financieros y deja vacíos normativos en orden a garantizar su completa protección". Cfr. Marcela Rojas Bejarano, "Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales", *Revista Novum Jus*, Nro. 1 (2014), ISSN 1692-6013, 107-139.

[80] Tovar, "Positivación y Protección de los Derechos Humanos: Aproximación Colombiana", 64.

[81] La Ley Estatutaria 1581, por la cual se dictan disposiciones generales para la protección de datos personales, entró en vigencia el 17 de octubre de 2012, mediante su publicación en el Diario Oficial

Ley "ha significado un adelanto importante en torno a la protección de cualquier dato personal que sea administrado por entidades públicas y privadas, de acuerdo con los principios generales establecidos en la Constitución"[82].

Hay que tomar en cuenta que, en este país, los mecanismos de control y respeto del derecho a la protección de datos personales "no dependen solo de los jueces, sino de la institución administrativa facultada o designada para ejercer eficiente control y vigilancia a los sujetos de derecho público y privado encargados del manejo de datos personales"[83]. Por ello, destacamos que la Ley 1581 estipula que la autoridad de control es la Superintendencia de Industria y Comercio, a través de una Oficina o Delegación para la Protección de Datos Personales[84]. Su objetivo es el respeto de los principios, derechos, garantías y procedimientos previstos en el marco de protección de la información de carácter personal.

Como sabemos, en el contexto internacional, la previsión de un organismo de control es fundamental, puesto que, "se considera necesaria la existencia de una autoridad independiente que no sólo controle, vigile y sancione a los que poseen datos personales, sino que reciba las quejas de los ciudadanos e inicie las investigaciones pertinentes con miras a que se convierta en un garante de la protección de estos datos"[85]. Para este fin, también es necesario "un verdadero compromiso ético por parte de quienes administran datos personales (administrador

48587. El ámbito de aplicación de esta Ley señala que: "Los principios y disposiciones contenidas en la presente Ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. La presente Ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales" –art. 2–.

[82] Lucero Galvis Cano, "Protección de datos en Colombia, avances y retos", *Revista Lebret de la Universidad Santo Tomás*, Nro. 4. (2012), 195-214.

[83] Rojas Bejarano, "Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales", 119.

[84] En este caso, la Ley Estatutaria 2581 dispone que: "La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley" –art. 19–.

[85] Nelson Remolina, "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?", *International Law: Revista Colombiana de Derecho Internacional*, Nro. 16 (2010): 489-524.

de datos) para que en su actividad no amenacen ni lesionen los derechos humanos"[86]. Precisamente, a partir de la Ley 1581, estas facultades han sido atribuidas a la Superintendencia de Industria y Comercio –arts. 17 y 18–. Su gestión se encamina a ejercer funciones de control, recepción de denuncias e inicio de investigaciones administrativas, con el objeto de establecer compromisos éticos en los responsables del tratamiento; y responsabilidades derivadas del incumplimiento del régimen jurídico previsto para la protección de los datos personales.

A pesar de no ser considerado por la Unión Europea como un país con un nivel adecuado para la protección de datos, el ordenamiento jurídico colombiano cuenta con el reconocimiento internacional de su autoridad de protección de datos otorgada por la "Conferencia Internacional de Comisionados de Protección de Datos y Privacidad"[87]. Asimismo, en noviembre de 2016, dicha autoridad fue llamada a integrar el Comité Ejecutivo de la Red Iberoamericana de Protección de Datos Personales (RIPD). En la actualidad, esta autoridad ostenta la presidencia de la RIPD, la cual es ejercida por la Superintendencia de Industria y Comercio.

En lo que corresponde a la jurisprudencia de la Corte Constitucional, una de las primeras resoluciones es la Sentencia de Tutela Nro. 175/95, que sobre el *habeas data* señala:

> El derecho al *habeas data*, consagrado en el artículo 15 de la C P, constituye un derecho fundamental claramente diferenciado del derecho a la intimidad y el buen nombre. La jurisprudencia constitucional ha delimitado el alcance del derecho al *habeas data*: "Cuál es el núcleo esencial del *habeas data*? A juicio de la Corte, está integrado por el derecho a la autodeterminación informática y por la libertad, en general, y en especial económica.

Ampliando este criterio, la Sentencia de Tutela Nro. 552/97 considera que:

---

[86] Nelson Remolina, "Data Protection: Riesgos y Desarrollos (Énfasis en el caso colombiano)", *Revista Chilena de Derecho Informático*, Nro. 7 (2005), 111-134.

[87] La Conferencia Internacional constituye un foro de encuentro, intercambio y discusión. Es una entidad que representa a los miembros acreditados. La condición de miembro de la Conferencia exige que las autoridades de control y supervisión cumplan una serie de requisitos, entre los que se incluyen: a) Constituir una entidad pública creada mediante instrumento legal; b) Tener supervisión de normas específicas de protección de datos; c) Que la legislación sea compatible con los instrumentos internacionales para la protección de datos; d) Disponer de facultades legales para ejercer sus funciones; y e) Contar con autonomía e independencia en el ejercicio de sus funciones. Cfr. International Conference of Data Protection and Privacy Commissioners. Disponible en: https://privacyconference2019.info/accredited-members-and-observers-2/.

> No obstante, y a pesar de que en determinadas circunstancias el derecho a la intimidad no es absoluto, las personas conservan la facultad de exigir la veracidad de la información que hacen pública y del manejo correcto y honesto de la misma. Este derecho, el de poder exigir el adecuado manejo de la información que el individuo decide exhibir a los otros, es una derivación directa del derecho a la intimidad, que se ha denominado como el derecho a la "autodeterminación informativa".

Finalmente, en relación a la protección de datos como un derecho fundamental autónomo, la Sentencia de Inconstitucionalidad Nro. 336/07 precisa:

> La jurisprudencia actual de la Corte ha deducido de los enunciados normativos del artículo 15 de la Constitución, la existencia y validez de tres derechos fundamentales constitucionales autónomos: el derecho a la intimidad, el derecho al buen nombre y el derecho al *habeas data*. (…) En cuanto al derecho fundamental al *habeas data* o a la autodeterminación informática, en diversas oportunidades la jurisprudencia de esta Corporación se ha referido a la naturaleza fundamental de este derecho, el cual comporta un plexo de facultades tales como la de disponer de la información sobre sí mismo, la de preservar la propia identidad informática, es decir, permitir, controlar o rectificar los datos concernientes a la personalidad del titular de los mismos y que, como tales, lo identifican e individualizan ante los demás.

La regulación del derecho a la protección de datos personales ubica a Colombia como uno de los países que merece reconocimiento internacional. “Cuenta con una regulación general e integral sobre la protección de datos personales y el tratamiento de los mismos con el desarrollo de los derechos constitucionales a la intimidad y sus diversas manifestaciones”[88]. Este país garantiza, desde el ámbito constitucional, sectorial e institucional una protección integral del derecho a la autodeterminación informativa. Por ello, se espera que sea “calificada como un país que garantiza un “nivel adecuado de protección” para así recibir información personal proveniente de la Unión Europea y los Estados Unidos, entre otros”[89].

### **2.1.5** Paraguay

El ordenamiento constitucional de este país no contempla un derecho relativo a la protección de datos. Al igual que la mayoría de los países latinoamericanos, la información de carácter personal se encuentra garantizada en la Constitución de

[88] Rojas Bejarano, “Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales”, 120.
[89] Galvis Cano, “Protección de datos en Colombia, avances y retos”, 205.

1992, mediante el "derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas" –art. 33–; y además, en las facultades de control de la información que permite ejercer el *habeas data* –art. 135–[90].

En este contexto, apuntamos que el *habeas data:*

> Garantiza a toda persona el acceso a las informaciones y datos sobre sí misma o sobre su patrimonio que se encuentren en registros oficiales o privados de público acceso. Así mismo, toda persona está legitimada para conocer el empleo o los fines de esas informaciones y datos, así como para solicitar ante el juez competente, en caso de error o cuando se viole un derecho de la persona, su actualización, corrección o destrucción[91].

Por una parte, la Ley Nro. 1.682/01 –modificada, posteriormente, por la Ley Nro. 1.969– reglamentaba el tratamiento de datos personales y garantizaba el ejercicio de los derechos de los titulares[92]. Si bien se trataba de una norma que regulaba el tratamiento de la información, ésta no contenía las disposiciones necesarias para que fuera considerada como una Ley General. Así, por ejemplo, en su contenido no se desarrollaban principios, garantías o mecanismos de protección, por medio de la actuación de una autoridad de control. Y por otra, mediante el Acuerdo 83 de la Corte Suprema de Justicia, se creó la Mesa de Entrada de Garantías Constitucionales para el sorteo y distribución de expedientes relativos a la garantía del *habeas data*[93]. Por tanto, habiéndose fijado, además, la competencia en los

---

[90] La Constitución de 1992 reconoce la protección de: "La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables. La conducta de las personas, en tanto no afecte al orden público establecido en la Ley o a los derechos de terceros, estará exenta de la autoridad pública. Se garantizan el derecho a la protección de la intimidad, de la dignidad y de la imagen privada de las personas" –art. 33–. Asimismo, garantiza que: "Toda persona podrá acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos" –art. 135–.

[91] Norbert Losing, "La justicia constitucional en Paraguay y Uruguay", en *Anuario de Derecho Constitucional Latinoamericano*, (Montevideo-Uruguay: Konrad-Adenauer-Stiftung, 2002), 120.

[92] La Ley Nº 1.682/01 refiere que: "tiene por objeto regular la recolección, almacenamiento, distribución, publicación, modificación, destrucción, duración y en general, el tratamiento de datos personales contenidos en archivos, registros, bancos de datos o cualquier otro medio técnico de tratamiento de datos públicos o privados destinados a dar informes, con el fin de garantizar el pleno ejercicio de los derechos de sus titulares" –art. 1–.

[93] El art. 2 del Acuerdo y Resolución 83 de la Corte Suprema de Justicia señaló que: "El sorteo y la distribución de los expedientes se realizará a través de un Sistema Informático denominado ´Sistema de Distribución de Expedientes de Garantías Constitucionales´, por el cual se dará entrada al expediente y al mismo tiempo se procederá al sorteo del juzgado de primera instancia interviniente en cada uno de ellos, sin perjuicio de las facultades propias de la Corte Suprema de Justicia en los pedidos de hábeas corpus".

Juzgados de primera instancia, existen algunas resoluciones que en materia de protección de datos son importantes destacar.

Sobre la naturaleza del *habeas data*, la Sentencia 148 de 5 de octubre de 2005 considera que:

> Conforme se puede valorar, el *Habeas data* constituye una acción que tiene como objetivo fundamental el acceso de las personas a los datos a ellas referidas, controlar su veracidad y rectificarlos o suprimirlos en casos de ser errados, incompletos o falsos, de donde se desprende que éste es un derecho constitucional reconocido, y la misma como garantía busca su efectiva protección ante dichas circunstancias.

En lo que respecta al ejercicio de las facultades de control, la Sentencia 74, de 9 de septiembre de 2005 señala que:

> En estas condiciones, el Juzgado concluye que corresponde hacer lugar a la presente acción de *Habeas data*, en consecuencia, deberá oficiarse al Departamento de Identificaciones a fin de que rectifique los datos del actor y se abstenga de consignar en el prontuario del mismo los datos o antecedentes judiciales de cualquier otra persona que no sea el actor.

En este mismo orden, la Sentencia 86, de 9 de julio de 2008 precisa que el *habeas data* "faculta a la actora a solicitar la destrucción, la actualización y rectificación de los datos erróneos que existan sobre su persona o sobre sus bienes".

Ahora bien, la Corte Suprema –como tribunal de apelación– ha desarrollado significativos criterios en relación a la protección de datos personales. Por ejemplo, el Acuerdo y Sentencia 5, de 1 de febrero de 2005, sobre la naturaleza del *habeas data*, expone que:

> El objeto de ésta Institución es la persona (en su fuero íntimo, en su ámbito privado) y sus bienes (entendido como reserva y completitud), los ciudadanos debemos conocer el uso y destino dado a la información o dato sobre nuestras personas y bienes. Esto nos permite, a través de la garantía constitucional, solicitar ante el órgano judicial competente la ACTUALIZACIÓN, LA RECTIFICACIÓN O SUPRESIÓN de aquellos, considerados erróneos o que afectaren ilegítimamente nuestros derechos. Los términos atizados por la Constitución; "INFORMACIÓN" refiera a la acción y efecto de enterar, instruir, y "DATO" a los antecedentes que permiten llegar más fácilmente a conocimiento de una cosa (…) La acción de *Habeas data* debe, necesariamente, ajustarse a los siguientes requisitos: a) Debe tratarse de una información y datos sobre las personas o sus bienes; b) La información o datos sobre requeridos deben constar en registros oficiales o privados de carácter público; c) y que el acceso a la información cumpla la finalidad de conocer el uso y destino, para solicitar su actualización, rectificación o destrucción, si ésta información o dato fueran erróneos o afectasen ilegítimamente algún derecho.

Así también, respecto al contenido del derecho a la protección de datos, la misma Resolución estima que:

> El bien jurídico protegido lo constituye sustancialmente la veracidad de la información, en lo referente a la persona y sus bienes. En primer lugar, se busca proteger a los individuos contra la información falsa o incompleta. Por otra parte, el derecho a la protección de datos (…) constituye un plexo de derechos específicos (…) Estos derechos constituyen el derecho a conocer, el derecho a acceder a los datos o información, y el derecho de rectificar o destruir los mismos. En realidad, lo que preocupa es controlar la veracidad de la información y el uso de que ella se hace.

Bajo este marco, la Corte Suprema de Justicia ha advertido que "el nivel de protección que ofrece la legislación nacional –Ley Nº 1682/2001 y Ley Nº 1969/2002– es insuficiente, a efectos de que Paraguay se acredite como nación *"adecuada"* ante los organismos de la Unión Europea"[94]. Naturalmente, sobre la autoridad de control, la Corte ha agregado que "es imprescindible contar con un organismo administrativo que vele por el cumplimiento de las disposiciones legales"[95]. En todo caso, en este último año se destaca la promulgación de la Ley Nro. 6534 de protección de datos personales crediticios, la cual deroga, tanto la Ley Nro. 1682 como la Nro. 1969, e introduce un nuevo régimen de protección de datos personales en este ámbito sectorial[96]. Además, este sería el antecedente para que en abril de 2021 se presente ante el Congreso de Paraguay el proyecto de Ley de Protección de Datos Personales

### **2.1.6** Perú

La Constitución de 1993 reconoció a la protección de datos personales, en virtud de los posibles riesgos que la tecnología representa en el tratamiento de la información de carácter personal. Conforme a dispuesto en la Constitución, puede considerarse como uno de los primeros ordenamientos jurídicos en identificar a la libertad

[94] Corte Suprema de Justicia, "Protección de Datos Personales", en Víctor Núñez (coord.), (Asunción – Paraguay: División de Investigación, Legislación y Publicaciones – Centro Internacional de Estudios Judiciales, 2010), 7.
[95] Ibíd., 8.
[96] La Ley Nro. 6534 entró en vigencia en octubre de 2020. Si bien se trata de una norma sectorial, en el ámbito crediticio su contenido desarrolla definiciones; principios; derechos de los titulares; e incorporación de una autoridad de control. Todo ello está enmarcado en un objeto, claramente, establecido, es decir, "garantizar la protección de datos crediticios de toda persona, cualquiera sea su nacionalidad, residencia o domicilio" –art. 1–.

informática como un derecho que nace de la facultad de controlar –en el ámbito público y privado– el tratamiento de la información en el mundo de las tecnologías de la información y comunicación[97].

Al respecto, destacamos que:

> El artículo 2°, inciso 7) de la Carta Constitucional reconoce los derechos a la intimidad, al honor y a la propia imagen, que ya se encontraban consagrados en la Constitución Política de 1979. En el mismo artículo 2°, pero en el inciso 6), se reconoce un nuevo derecho, cuando señala que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. El Tribunal Constitucional definió este derecho como el de autodeterminación informativa, en su sentencia de fecha 29 de enero de 2003, expediente Nº 1797-2002-HD/TC, en el marco de un proceso de *habeas data*[98].

La base para el desarrollo del derecho a la autodeterminación informativa, precisamente, fue el reconocimiento constitucional de la libertad informática, a partir de las facultades de control de la información que garantiza el *habeas data*. Así, la Constitución de 1993 caracterizó al *habeas data* como un medio procesal de tutela, no solamente del derecho a la protección de datos sino también de los derechos a la intimidad y a la imagen propia –art. 200.3–[99]. Por ello, esta Constitución establecía "los derechos que constituyen la fuente primigenia que marca e inspira la legislación existente sobre protección de datos personales"[100].

En todo caso, la reforma de 1995 –que afectó a la disposición constitucional anteriormente señalada–, permitió desvincular del *habeas data* la protección de los

[97] La Constitución de 1993 reconoce el derecho a: "solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por Ley o por razones de seguridad nacional" –art. 2.5–; "que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar" –art. 2.6–; y "al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de Ley" –art. 2.7–.

[98] María de Lourdes Zamudio, "El marco latinoamericano y Ley de Protección de Datos Personales en Perú", *Revista Internacional de Protección de Datos Personales*, Nro. 1 (2012), ISSN: 2322-9705.

[99] En este ámbito, la Constitución de 1993 refería que el *habeas data* "procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2º, incisos 5, 6 y 7 de la Constitución" –art. 200.3–.

[100] Zamudio, "El marco latinoamericano y Ley de Protección de Datos Personales en Perú". 10.

derechos relacionados con el honor; la buena reputación, la intimidad personal y familiar y la imagen propia[101]. En este sentido, afirmamos que:

> El artículo 200º, inciso 3) de la Constitución Política de 1993, establece la Garantía Constitucional del *habeas data* para proteger los derechos reconocidos en los incisos 5), derecho de acceso a la información pública, y 6) derecho a la protección de datos personales, del artículo 2º de la Carta fundamental[102].

Ahora bien, la Ley 29733 de 2011 sobre datos personales desarrolla el contenido del derecho a la protección de datos. El objeto de esta Ley se enmarca en garantizar este derecho fundamental reconocido en la Constitución[103]. De esta manera, "se ´coloca´ legalmente el epígrafe al citado numeral constitucional, definido en algunas oportunidades por la jurisprudencia del Tribunal Constitucional como el derecho a la autodeterminación informativa"[104].

Como hemos advertido, la relevancia que tiene la incorporación de una autoridad administrativa es necesaria dentro del sistema de protección de datos. El art. 32 de la Ley 29733 dispone que el Ministerio de Justicia (hoy, Ministerio de Justicia y Derechos Humanos), mediante la Dirección General de Protección de Datos Personales (DGPDP) se constituye como una autoridad de control[105]. Así, respecto a la naturaleza de esta autoridad, en primer término, interpretamos que:

> No encontramos en la Ley, en el proyecto de Reglamento ni en el Reglamento de organización y funciones del Ministerio, referencia explícita sobre el nivel de autonomía o de independencia técnica de la Autoridad; pero sí es explícito que ella será ejercida por una

[101] Mediante la Ley Nro. 26470, publicada el 12 de junio de 1995, se modifica el art. 200.3 de la Constitución Política de Perú. Esta nueva disposición prescribe que el *habeas data* es una garantía constitucional que "procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el artículo 2, incisos 5 y 6 de la Constitución".

[102] Zamudio, "El marco latinoamericano y Ley de Protección de Datos Personales en Perú", 11.

[103] La Ley 29733 reconoce como su objeto que "garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen" –art. 1–.

[104] Zamudio, "El marco latinoamericano y Ley de Protección de Datos Personales en Perú". 12.

[105] Tal como lo indica la Ley 29733: "Corresponde a la Autoridad Nacional de Protección de Datos Personales realizar todas las acciones necesarias para el cumplimiento del objeto y demás disposiciones de la presente Ley y de su reglamento. Para tal efecto, goza de potestad sancionadora, de conformidad con la Ley 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces, así como de potestad coactiva, de conformidad con la Ley 26979, Ley de Procedimiento de Ejecución Coactiva, o la que haga sus veces" –art. 32.3–.

> Dirección General, que si bien es cierto tiene competencia nacional, es un órgano de tercer nivel dependiente de un viceministerio[106].

Dada las críticas, con relación a la independencia de la autoridad de control, en esta parte, también es conveniente advertir que:

> Es esta independencia la que favorece la confianza de los administrados, confianza especialmente necesaria cuando lo que se está aplicando son normas jurídicas con abundantes conceptos jurídicos indeterminados. (…) Dada la dificultad para el control judicial de la discrecionalidad técnica de la Administración, es aconsejable que exista una Administración Independiente para la protección de datos personales, cuyos miembros dispongan de la especialidad técnica necesaria para que tutelen el derecho fundamental de manera previa a la revisión de los órganos jurisdiccionales. Tanto la independencia como la competencia técnica favorecen la confianza de los sectores regulados[107].

La independencia de la autoridad administrativa es una exigencia del principio de "confianza" de los administrados en la Administración Pública, que exige garantizar la imparcialidad en el conocimiento, control y sanción de la vulneración de los derechos fundamentales afectados por el tratamiento de la información de carácter personal. Por ello, agregamos que:

> Si bien la ANPDP es una entidad pública de carácter administrativa cuya existencia no emana de la Constitución sino de una ley, resulta bastante discutible la justificación y conveniencia de la decisión de la LPDP de atribuirle este rol a una entidad subalterna ubicada al interior de la estructura del Ministerio de Justicia. Y no sólo porque ello puede afectar sus niveles reales de autonomía, aspecto ciertamente delicado por tratarse de una instancia que debe controlar el respeto de un derecho constitucional como la protección de los datos personales, sino porque la Dirección a la que se integra tiene un conjunto recargado de funciones ordinarias y limitaciones operativas o presupuestales que dificultan su adecuado desarrollo y proyección[108].

La importancia de una autoridad independiente para la protección de datos personales es trascendental. En su organización, la DGPDP de Perú se encuentra adscrita al Ministerio de Justicia y Derechos Humanos y se compone de cuatro Direcciones, a saber: Dirección de Registro Nacional de Protección de Datos Personales, Dirección de Supervisión y Control, Dirección de Normatividad y Asistencia Legal y Dirección de Sanciones. En todo caso, la desaprobación de que dependa del Ministerio de Justicia estaría justificada en la exposición de motivos de la ahora Ley de Protección de Datos Personales.

---

[106] Zamudio, "El marco latinoamericano y Ley de Protección de Datos Personales en Perú". 17.
[107] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1729-1730.
[108] Francisco Eguiguren Praeli, "El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú", *THĒMIS-Revista de Derecho* Nro. 67 (2015),131-140.

Con referencia a este aspecto, apuntamos que:

> Según la exposición de motivos del Proyecto de Ley 4079-2009-PE –Ley de Protección de Datos Personales–, el fundamento para adscribir a la Autoridad Nacional de Protección de Datos Personales al Ministerio de Justicia y Derechos, encontraría sustento en la situación de austeridad que atravesaba el país en el momento de la redacción de tal documento[109].

Por otra parte, la DGPDP –de conformidad a la segunda disposición complementaria de la Ley 27933–, en su actividad de control y supervisión ha desarrollado la Directiva de Seguridad de la Información, que tiene por objeto garantizar la seguridad de los datos personales contenidos o destinados a ser incluidos en bancos de datos de información personal. Así también sus resoluciones se orientan a regular el flujo transfronterizo de datos, los formularios de inscripción de bancos de datos y formularios de denuncias, entre otros. Por tanto, consideramos que estas actividades han permitido garantizar, adecuadamente, el derecho a la protección de datos. Su modelo de supervisión está destinado a controlar el tratamiento de la información en el ámbito público y privado. De igual manera, fiscalizar el cumplimiento de la normativa; tramitar procedimientos administrativos y sancionadores, según las Directivas y Resoluciones técnicas y jurídicas, las cuales evidencian el compromiso que exige este derecho fundamental.

Ahora bien, la jurisprudencia del Tribunal Constitucional ha sentado algunos criterios sobre el derecho a la autodeterminación informativa. Por ejemplo, la Sentencia 71797-2002 apunta que:

> El derecho reconocido en el inciso 6) del artículo 2° de la Constitución es denominado por la doctrina *derecho a la autodeterminación informativa* y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7) del mismo artículo 2° de la Constitución. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen (…) En ese sentido, por su propia naturaleza, el derecho a la autodeterminación informativa, siendo un derecho subjetivo tiene la característica de ser, *prima facie* y de modo general, un derecho de naturaleza relacional, pues las exigencias

[109] Héctor Figari y María del Carmen Quiroz, “La protección de datos personales: Una herramienta para promover la inversión”. *THĒMIS-Revista de Derecho* Nro. 61 (2012),125-140.

> que demandan su respeto, se encuentran muchas veces vinculadas a la protección de otros derechos constitucionales.

Esta misma Sentencia, sobre el *habeas data* agrega:

> Este Tribunal ha expresado en la sentencia recaída en el Exp. N°. 666-1996-HD/TC que la protección del derecho a la autodeterminación informativa a través del *habeas data* comprende, en primer lugar, la capacidad de exigir jurisdiccionalmente la posibilidad de acceder a los registros de información, computarizados o no, cualquiera que sea su naturaleza, en los que se encuentren almacenados los datos de una persona (…) Asimismo, con el derecho en referencia, y en defecto de él, mediante el *habeas data*, un individuo puede rectificar la información, personal o familiar, que se haya registrado; impedir que esta se difunda para fines distintos de aquellos que justificaron su registro o, incluso, tiene la potestad de cancelar aquellos que razonablemente no debieran encontrarse almacenados.

El ordenamiento jurídico de este país ha desarrollado un destacado modelo de regulación y tutela sobre el derecho a la protección de datos. La protección constitucional ha evolucionado, desde la amplitud del derecho a la intimidad, hasta el reconocimiento del derecho a la libertad informática. De la jurisprudencia citada (2002), la autonomía del derecho a la autodeterminación informativa ha sido lograda con anterioridad a la entrada en vigencia de la Ley de Protección de Datos Personales en 2011. Queda pendiente, considerar la separación de la autoridad de control del Ministerio de Justicia y Derechos Humanos. Por un lado, se insiste en que "debe revisarse la ubicación dentro del aparato estatal y del Poder Ejecutivo que le ha asignado la LPDP, a fin de dotarla y garantizarle adecuados niveles de autonomía funcional y proyección institucional, acordes con los estándares internacionales"[110]; y por otro, se señala que "la realidad económica ha cambiado, por lo cual se debería evaluar la posibilidad de crear un ente independiente"[111].

Pese a la crítica sobre la independencia de la autoridad de protección de datos, la DGPDP ha ejecutado las acciones necesarias que una autoridad de control por vía administrativa e independiente debe ejecutar, para el cumplimiento del objeto y demás disposiciones relacionadas con el derecho a la autodeterminación informativa. Por ello, conviene destacar que, como autoridad de control, la DGPDP

[110] Eguiguren Praeli, "El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú", 140.
[111] Figari y Quiroz, "La protección de datos personales: Una herramienta para promover la inversión", 140.

se encuentra reconocida por la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad[112].

### **2.1.7** Venezuela

La Constitución de 1999 garantiza la protección de la información personal, mediante algunas disposiciones relativas al control de los datos[113]. Así, se reconoce el derecho a acceder a la información personal que conste en registros públicos o privados; conocer el uso y finalidad de los datos; y ejercer el derecho a la actualización, rectificación y destrucción en el caso de que la información resulte errónea o afecte algún derecho fundamental –art. 28–.

Como hemos señalado en otro momento, algunas previsiones constitucionales sobre el *habeas data* –también en el caso de Venezuela– tienden a confundir el derecho de acceso, como parte del derecho fundamental a la protección de datos, con el derecho de acceso a la información pública. En este sentido, subrayamos que el derecho de acceso a la información pública acredita un contenido más amplio y distinto del derecho de acceso como facultad del derecho fundamental a la protección de datos personales. Así, nos referimos a que el objeto del derecho de acceso a la información pública "excede de los datos de carácter personal sometidos a tratamiento, el origen de dichos datos y las comunicaciones realizadas o que se prevén hacer de los mismos (…) aplicándose en todo caso los límites relativos a la protección de datos personales"[114]

> Resulta en efecto imprescindible aclarar la relación existente entre transparencia y protección de datos, sobre todo teniendo en cuenta que la transparencia es capital para el

[112] Cfr. International Conference of Data Protection and Privacy Commissioners. Disponible en: https://privacyconference2019.info/accredited-members-and-observers-2/.

[113] La Constitución de 1999 reconoce que: "Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la Ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos" –art. 28–.

[114] Antonio Troncoso, "La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>", en Antonio Troncoso (Dir.), *Comentario a la Ley de transparencia, Acceso a la Información Pública y Buen Gobierno*, (Navarra, Aranzadi, 2017), 1058, 1059.

> desarrollo de una sociedad abierta y democrática, y que el respeto a la protección de datos no debe considerarse un obstáculo al derecho de acceso a la información a la información, pero sin olvidar que una de las excepciones que pueden invocarse al ejercer el derecho de acceso es la derivada del derecho a la protección de datos o de la existencia de información o documentos que afecten a la intimidad de las personas[115].

Si bien la naturaleza del *habeas data* está dirigida a garantizar las facultades de control de la información personal –y, a su vez, imponer prohibiciones en el tratamiento–, es preciso diferenciar que el "derecho a la información pública tiene como fin la transparencia de la gestión pública; la finalidad del *habeas data* es la de garantizar el derecho fundamental a la intimidad de los ciudadanos, concretado en la protección de sus datos personales"[116]. Por ello, insistimos en que el derecho de acceso –como parte del derecho fundamental a la protección de datos– tiene un contenido más limitado que el derecho de acceso a la información pública. Es decir, el derecho de acceso a la información pública es mucho más amplio y permite, no sólo acceder a datos personales sino también a documentos que obren en archivos administrativos o formen parte de un expediente[117].

Hechas estas salvedades, también advertimos que la Constitución garantiza que la Ley "limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos" –art. 60–[118]. Considerando a la protección de la intimidad, frente al uso de la informática

---

[115] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 161-162. En todo caso, como advierte Antonio Troncoso, el derecho de acceso -como facultad del derecho fundamental a la protección de datos personales- "se limita a lo establecido en la normativa de protección de datos personales mientras que el derecho de acceso a la información pública se extiende al contenido de la información pública –que es más amplio que el anterior–". Cfr. Troncoso, "La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>", 1059.

[116] Ibíd., 118-119.

[117] Cfr. Antonio Troncoso, "La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>", 1056-1060.

[118] La Constitución de 1999 determina que: "Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos" –art. 60–. Sobre los derechos reconocidos en los arts. 28 y 60 de la Constitución de Venezuela, la protección de datos personales sigue sin tener un reconocimiento expreso, tomando en cuenta la versión más reciente de la Constitución Venezolana que fue sancionada por la Asamblea Nacional el 14 de enero de 2009 y promulgada el 19 de febrero de 2009.

como un derecho civil[119]; con un texto constitucional, idéntico al español, nos parece que el legislador debió tomar como referencia los criterios doctrinarios –incluso, como se verá más adelante, observando la experiencia de España–, que han sido desarrollados sobre la disposición, anteriormente, citada.

Desde esta perspectiva, debería incluirse, en el texto constitucional, un derecho fundamental autónomo, que compartiera con el derecho a la intimidad la protección integral de la vida privada personal y familiar. Por tanto, advertimos que "el nuevo derecho a la protección de datos, demanda garantías propias (judiciales y extrajudiciales) que permitan su plena vigencia; papel que hasta la fecha se ha dejado en manos del *habeas data*, pretendiendo que él únicamente resuelva un sinnúmero de situaciones"[120].

Tomando como referencia este reconocimiento constitucional, la Sentencia Nro. 323 del Tribunal Supremo de Justicia precisa que:

> El artículo 28 de la vigente Constitución establece el derecho de las personas a conocer la información que, sobre ellas, hayan sido compiladas por otras. Dicha norma reproduce un derecho reconocido en varios países como Suecia, Noruega, Francia y Austria, entre otros (…) la Constitución, para controlar tales registros, otorga varios derechos a la ciudadanía que aparecen recogidos en el artículo 28 citado. Estos derechos son: 1) El derecho de conocer sobre la existencia de tales registros. 2) El derecho de acceso individual a la información, la cual puede ser nominativa, o donde la persona queda vinculada a comunidades o a grupos de personas. 3) El derecho de respuesta, lo que permite al individuo controlar la existencia y exactitud de la información recolectada sobre él. 4) El derecho de conocer el uso y finalidad que hace de la información quien la registra. 5) El derecho de actualización, a fin que se corrija lo que resulta inexacto o se transformó por el transcurso del tiempo. 6) El derecho a la rectificación del dato falso o incompleto. 7) El derecho de destrucción de los datos erróneos o que afectan ilegítimamente los derechos de las personas.

Si bien no se hace una referencia taxativa, como un derecho específico a la protección de datos personales, existe un reconocimiento expreso de otros bienes

[119] Llama la atención la similitud del texto constitucional venezolano, con el art. 18.4 del texto constitucional español. Si bien, la Constitución de España señala que "la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", la diferencia más significativa es que, mientras la Constitución de España lo hace como un "derecho y libertad", Venezuela lo caracteriza como un "derecho civil". Así también en el texto constitucional de Venezuela incluye la palabra "ciudadanas", bajo las prerrogativas de la inclusión de género, en la denominada democracia participativa.

[120] Eligio Rodríguez Marcano, "El derecho fundamental a la protección de datos de carácter personal en Venezuela y su recorrido y reconocimiento desde la Sala Constitucional del Tribunal Supremo de Justicia de Venezuela", *Revista Latinoamericana de Protección de Datos Personales*, Nro. 1 (2015), ISSN 2422-6769.

jurídicos que se protegen, a partir del tratamiento de la información y que se tutelan, mediante la garantía del *habeas data*. En todo caso, la Sentencia Nro. 1318 del Tribunal Supremo de Justicia ha considerado a la protección de datos personales como un derecho fundamental autónomo. Así, en lo correspondiente señala:

> La Constitución de la República Bolivariana de Venezuela, recoge la protección de datos de carácter personal, la cual se constituye en un derecho fundamental autónomo que subyace en el contenido de los artículos parcialmente transcritos y que tiene como finalidad cardinal, permitir que todas las personas puedan controlar el acceso y uso por terceros de sus datos personales y, a su vez, que evitar los datos de carácter personal recogidos sufran desviaciones de la finalidad para la que fueron recabados.

Además, sobre el objeto del derecho a la autodeterminación informativa, esta Sentencia agrega que:

> En este sentido, se ha pronunciado la doctrina cuando entiende que la libertad informática y el derecho a la autodeterminación informativa, son en cierto modo sinónimos, ya que constituyen un nuevo derecho fundamental que tiene por objeto garantizar la facultad de las personas para conocer y acceder a las informaciones que les conciernen archivadas en base de datos, controlar su calidad o que impliquen la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados; y disponer sobre su transmisión.

Por otra parte, en el régimen sectorial, las normas que regulan los derechos conexos a la protección de datos personales son la “Ley sobre protección a la privacidad de las comunicaciones” y la “Ley sobre mensajes de datos y firmas electrónicas”. El objeto de estas nomas se dirige a proteger la privacidad, la confidencialidad y el secreto de las comunicaciones y la regulación del acceso a la información personal por medios telemáticos. Debido a la ausencia de un marco de regulación específico para la protección de datos, se aprecia la falta de una autoridad de control, la cual, según entiende la doctrina venezolana, “comprende las facultades de control y seguimiento y que tienen incidencia en el tratamiento (oposición, actualización, rectificación e incluso la indemnización)”[121].

En todo caso, la Constitución reconoce que el Defensor del Pueblo tiene la atribución de velar por el efectivo respeto y garantía de los derechos fundamentales consagrados en la Constitución; y, además, puede interponer acciones de *habeas data* como resultado de investigaciones de oficio o por requerimiento de parte –art. 281 –. Conviene señalar que –con referencia anterior, se acredita que el problema

[121] Ibíd.

del Defensor del Pueblo es si controla tanto los ficheros privados como los públicos, y si sobre ellos tiene o no potestad sancionadora–. Según lo dispuesto por la Ley Orgánica de la Defensoría del Pueblo, uno de los objetivos de la Defensoría es la promoción, defensa y vigilancia de "los derechos, garantías e intereses de todas las personas en relación con los servicios públicos, sea que fueren prestados por personas jurídicas públicas o privadas" –art. 4–. Por la mencionada Ley, el Defensor del Pueblo tiene derecho a interponer o adherirse a las acciones del *habeas data,* con el objeto de solicitar ante el órgano competente la aplicación de correctivos y sanciones por los derechos consagrados en la Constitución –art. 15–.

Sobre su actividad en materia de protección de datos, se considera que "es interesante como el Defensor del Pueblo, delata que las instituciones financieras, por vía del artículo 192 del Decreto N° 1.526 con Fuerza de Ley de Reforma de la Ley General de Bancos y Otras Instituciones Financieras y con base a los artículos 1, 6 y 8 de la Resolución N° 001-06-98, del 26 de junio de 1998, vulneran el artículo 28 y 60 de la Constitución"[122]. Así, asumimos que el Defensor del Pueblo actúa como una "autoridad de control", con potestades jurisdiccionales para supervisar que el tratamiento de la información personal –tanto en el ámbito público como privado– cumpla con lo dispuesto en la Constitución. No obstante, no tiene potestad sancionadora, por cuanto, únicamente, puede recomendar algún tipo de sanción.

Bajo estas consideraciones, el ordenamiento jurídico venezolano presenta algunas limitaciones en el desarrollo de un marco jurídico adecuado, para la protección de datos personales. Por ejemplo, se debe considerar que en el texto constitucional de Venezuela no existe una definición específica acerca del *habeas data*[123], a pesar de que según la jurisprudencia la asocia como una garantía constitucional contenida

[122] Ibíd.

[123] Sin embargo, en la exposición de motivos de la Constitución de 2009 se hace referencia al siguiente texto: "Se reconoce por vez primera en el constitucionalismo venezolano, el *habeas data* o el derecho de las personas de acceso a la información que sobre sí mismas o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la Ley. El *habeas data* incluye el derecho de las personas de conocer el uso que se haga de tales registros y su finalidad, y de solicitar ante el tribunal competente su actualización, rectificación o destrucción, si fuesen erróneos o afectasen ilegítimamente sus derechos".

en el artículo 28 de la Constitución[124]. A esto, se suma la ausencia de una Ley general que desarrolle el derecho a la protección de datos y la inexistencia de una autoridad de control independiente.

### **2.1.8** Bolivia

Inicialmente, la Constitución de 1967 garantizaba a la protección de la información personal, a partir del derecho a la inviolabilidad de las comunicaciones privadas. Su garantía estaba amparada en el derecho a la privacidad de la correspondencia y comunicaciones que prohibía la interceptación de la información, tanto a personas como entidades, de orden público y privado –art. 20–[125]. Así también la tutela de estos derechos estaba reconocida, mediante el recurso de amparo cuyo objeto, en sede judicial, preveía la protección contra actos ilegales u omisiones de funcionarios públicos y particulares –art. 19–[126].

Carente, incluso, de reconocer a la protección de la intimidad como un derecho fundamental, en el mejor de los casos, la Constitución aseguraba la protección de los datos personales, a partir del respeto de los derechos a la dignidad y de libertad. Posteriormente, la "Ley de Necesidad de Reforma a la Constitución 2410" introduce la reforma de los arts. 7 y 23 de la Constitución. Así, se reconoció como un derecho

[124] El Tribunal Supremo de Justicia, mediante Sentencia Nro. 323 ha señalado que: "Como se evidencia de la lectura de la norma, quien quiere hacer valer estos derechos (que conforman el *habeas data*), lo hace porque se trata de datos que le son personales, y ello mediante una acción que aún no ha desarrollado la Ley, lo que a juicio de esta Sala no impide –que mientras la Ley la establezca– se incoe mediante el recurso de amparo constitucional, si es que la infracción de los derechos que otorga el artículo 28 citado, lesionan la situación jurídica de las personas".

[125] La Constitución de 1967 señalaba que: "Son inviolables la correspondencia y los papeles privados, los cuales no podrán ser incautados sino en los casos determinados por las Leyes y en virtud de orden escrita y motivada de autoridad competente. No producen efecto legal los documentos privados que fueren violados o sustraídos. Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones y comunidades privadas mediante instalación que los controle o centralice" –art. 20–.

[126] Así también la Constitución de 1967 Bolivia determinaba que: "Se establece el recurso de amparo contra los actos ilegales o las omisiones indebidas de los funcionarios o particulares que restrinjan, supriman o amenacen restringir o suprimir los derechos y garantías de la persona reconocidos por esta Constitución y las Leyes. El recurso de amparo se interpondrá por la persona que se creyere agraviada o por otra a su nombre con poder suficiente ante las Cortes Superiores" –art. 19–.

fundamental a la intimidad y privacidad personal y familiar –art. 7–; y como una garantía constitucional al *habeas data* –art. 23–.

Ahora bien, luego de aprobarse la Constitución de 2009, se produce una significativa reforma, en materia de protección de datos. En primer término, se conceptualizó como un derecho civil a la intimidad –art. 21.2–[127] y segundo, se garantizó la protección de datos personales, mediante la acción de protección de privacidad –art. 130–[128]. Sobre la acción de privacidad, advertimos que significa "una acción que protege los datos personales (edad, sexo, enfermedad, pertenencia política, etc.) de cada quien, y que figuran en centros de identificación, registro electoral, registros médicos, sistemas bancarios, etc. Estos datos son de propiedad exclusiva de su titular"[129]. Y, asimismo, constituye "un proceso constitucional de naturaleza tutelar que tiene por finalidad la protección inmediata y efectiva del derecho a la 'autodeterminación informativa', restableciendo o restituyendo cuando este sea restringido o vulnerado de manera ilegal o indebida"[130].

En el ámbito sectorial, destacamos la Ley Nro. 164, la cual se destina a proteger las telecomunicaciones y tecnologías de la información y comunicación. Así, garantiza el "derecho humano individual" que busca asegurar la protección de datos personales desde el contexto tecnológico[131]. La reglamentación de esta Ley está contenida en el Decreto Supremo Nro. 1793. Dentro de los "aspectos generales" de este Decreto se desarrollan definiciones sobre datos personales, consentimiento y tratamiento de los datos. Como "principios", describe a la finalidad, veracidad,

[127] Esta reforma de la Constitución de 2009 introdujo el reconocimiento del derecho a: "la privacidad, intimidad, honra, honor, propia imagen y dignidad" –art. 21.2–.
[128] La Constitución de 2009 determina que: "Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad" –art. 130–.
[129] Idón Chivi Vargas, *Nueva Constitución Política del Estado: Conceptos fundamentales para su desarrollo normativo*, (La Paz – Bolivia: Vicepresidencia del Estado Plurinacional, 2010), 208.
[130] José Rivera Santivañez, *Jurisdicción Constitucional: Procesos constitucionales en Bolivia,* (Cochabamba – Bolivia, 2011), 433.
[131] En este aspecto, la Ley Nro. 164 reconoce como una obligación de los proveedores y operadores: "Brindar protección sobre los datos personales evitando la divulgación no autorizada por las usuarias o usuarios, en el marco de la Constitución Política del Estado y la presente Ley" –art. 59–.

transparencia, seguridad y confidencialidad. Y, en el Capítulo ll, reglamenta el tratamiento de los datos personales en el ámbito público y privado, considerando el respeto de los derechos fundamentales y garantías establecidas en la Constitución. Así también prevé que la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes sea una instancia de protección, supervisión y control. En este punto, es importante mencionar que, esta autoridad no ha desarrollado las funciones que corresponden a una autoridad de protección de datos. Por tanto, observamos la inexistencia de un órgano regulador para este fin.

En todo caso, conforme a lo dispuesto en la Constitución, la Defensoría del Pueblo tiene funciones relacionadas con la vigencia, promoción, difusión y cumplimiento de los derechos humanos –art. 218–[132]. Así, una importante atribución de este organismo es interponer las acciones de protección de privacidad, sin la necesidad de mandato y, además, receptar denuncias e iniciar investigaciones por acciones que impliquen la vulneración de derechos fundamentales –art. 222–. No obstante, no tiene potestad sancionadora y, únicamente, puede formular sugerencias para la reparación de los derechos.

Por otra parte, acerca del *habeas data* y autonomía del derecho a la protección de datos personales, la jurisprudencia del Tribunal Constitucional destaca en la Sentencia 965/2004 que:

> El *habeas data* es una garantía constitucional que tiene por objetivo el contrarrestar los peligros que conlleva el desarrollo de la informática en lo referido a la distribución o difusión ilimitada de información sobre los datos de la persona; y tiene por finalidad principal el proteger el derecho a la autodeterminación informática, preservando la información sobre los datos personales ante su utilización incontrolada, indebida e ilegal, impidiendo que terceras personas usen datos falsos, erróneos o reservados que podrían causar graves daños y perjuicios a la persona. El *habeas data* tiene la función primordial de establecer un equilibrio entre el "poder informático" y la persona titular del derecho a la autodeterminación informática, es decir, entre la entidad pública o privada que tiene la capacidad de obtener, almacenar, usar y distribuir la información sobre datos personales y la persona concernida por la información.

Asimismo, con relación a la reforma constitucional de 2009, el Tribunal en la Sentencia 496/2015 estima que:

[132] Según la Constitución, la función de la Defensoría del Pueblo "alcanzará a la actividad administrativa de todo el sector público y a la actividad de las instituciones privadas que presten servicios públicos" –art. 218–.

> En mérito al art. 61 del Código Procesal Constitucional (CPCo), la acción de protección de privacidad puede interponerse de manera directa sin trámite administrativo previo; además, protege el derecho a la autodeterminación informativa, el cual es activado cuando las personas que tienen a su cargo un banco de datos públicos o privados asumen una postura ilegal o indebida al no permitir el acceso, rectificación, corrección, eliminación o mantenimiento de datos (…) Se puede precisar que la acción de protección de privacidad, constituye una garantía constitucional de carácter procesal que puede ser interpuesta ante la jurisdicción constitucional -previo agotamiento de los medios administrativos o judiciales- por cualquier persona natural o jurídica que considere que se vulneran sus derechos a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación por estar impedida de obtener la eliminación o rectificación de sus datos personales registrados en cualquier archivo o banco de datos públicos o privados.

Evidenciamos que el marco jurídico boliviano ha pasado de un estado de regulación incierto a un sistema un poco más ordenado. No reconoce a la protección de datos como un derecho autónomo, pero determina al *habeas data* como una acción de protección para la privacidad de la información personal. Así también no cuenta con una Ley general que regule el derecho a la protección de datos. Aun así, la regulación del tratamiento de datos se afirma en algunas normas sectoriales. Si bien, por medio de este ordenamiento jurídico se promueve una autoridad de control, en la práctica no se evidencia un correcto ejercicio de las potestades que debe aplicar dicho organismo. Más bien, pueden atribuirse estas facultades a la Defensoría del Pueblo.

### **2.1.9** Chile

La Constitución de 1980, reformada por la Ley Nro. 21096 de junio de 2018, reconoce el respeto y protección "a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de esos datos se efectuará en la forma y condiciones que determine la Ley" –art. 19.4–[133]. Esta reforma constitucional fue considerada incompleta, toda vez que, como advierte Renato Jijena, ésta debía estar encaminada, tanto al reconocimiento del derecho a la protección de datos personales, así como también

[133] La reforma constitucional contemplaba lo siguiente: "Artículo único. Agrégase, en el numeral 4° del artículo 19 de la Constitución Política de la República, a continuación de la expresión " y su familia", lo siguiente: ", y, asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la Ley".

a la constitucionalización del *habeas data*, requiriéndose la necesidad de una autoridad autónoma que ejerza su protección[134].

Antes de la reforma propuesta en la Ley Nro. 21096, la protección de la información personal estaba vinculaba con el derecho a la intimidad y se garantizaba, mediante el recurso de protección[135]. En todo caso, el ejercicio de los derechos de acceso a la información personal, modificación, cancelación o bloqueo, ya se reconocían en la Ley Nro. 19.628 sobre la protección de la vida privada –art. 13–[136]. Dicha ley, considerada en la materia como la primera en América Latina[137], se orienta a regular el tratamiento de la información personal, tanto en al ámbito público como privado, a excepción de las libertades de opinión e información[138].

---

[134] En concreto, Jijena planteaba que la reforma haga en los siguientes términos: "Artículo único: Modificase el artículo 19 número 4 de la Constitución [...] agregándose los siguientes incisos segundo y tercero: Toda persona tiene derecho a la protección de sus datos personales, los que deben ser tratados para fines concretos y específicos, con su propio consentimiento, o en virtud de otro fundamento contemplado en la Ley, y tendrá, asimismo, derecho a acceder a dichos datos, para obtener su rectificación, actualización o cancelación, según procediere. Una Ley orgánica constitucional establecerá las normas para la debida aplicación de este derecho, como asimismo el órgano autónomo que velará por el cumplimiento de dicha Ley y controlará su aplicación". Cfr. Renato Jijena Leiva, "Tratamiento de Datos Personales en el Estado y acceso a la información pública", *Revista Chilena de Derecho y Tecnología*, Nro. 2 (2013), 49-94.

[135] En este aspecto, la Constitución señala que: "El que por causa de actos u omisiones arbitrarios o ilegales sufra privación, perturbación o amenaza en el legítimo ejercicio de los derechos y garantías establecidos en el artículo 19, números 1º, 2º, 3º inciso quinto, 4º, 5º, 6º, 9º inciso final (…) podrá ocurrir por sí o por cualquiera a su nombre, a la Corte de Apelaciones respectiva" –art. 20–.

[136] La Ley Nro. 19.628 reconoce que: "Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente. En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen. Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos. Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal" –art. 12–.

[137] Cfr. Pablo Palazzi, "Avances en la protección de datos personales en América Latina", *Revista Latinoamericana de Protección de Datos Personales*, Nro. 3 (2011), ISSN 2422-6769.

[138] La Ley 19628 sobre protección de datos de carácter personal refiere que: "El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta Ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la Ley a que se refiere el artículo 19, N° 12, de la Constitución Política. Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta Ley y para finalidades permitidas

Por una parte, el procedimiento especial de *habeas data* que plantea la Ley 19.628, en el art. 16, supone algunas problemáticas en el ejercicio del derecho a la protección de datos, por cuanto "si bien la ley reconoce una serie de derechos a las personas naturales titulares de los datos, estos deben ser ejercidos ante tribunales civiles, en procedimiento de larga y costosa tramitación, lo que constituye una barrera para el ciudadano común"[139]. Y por otra, existe gran debate en relación a la adecuación de la autoridad de control, regulación y tutela de este derecho fundamental. Así, la Ley Nro. 20285 sobre Acceso a la Información Pública señala que la autoridad, encargada de velar por el desarrollo de los derechos contemplados en la Ley de Protección de datos es el Consejo para la Transparencia[140].

Sobre este respecto, apuntamos que:

> Cuando la Ley 20.285 se refiere a las facultades de dictar instrucciones y recomendaciones declara explícitamente la dimensión en la que se puede mover el Consejo y en ella no queda comprendida la protección de datos. De ahí en adelante, y sin ese piso legal, lo que viene es ilegal. Lo establecido en el artículo 33 letra m) es una competencia limitada. Esta facultad no se puede extender al punto de considerar que estamos frente a la nueva Autoridad o Agencia de Protección de Datos chilena, y de creer que el Consejo posee competencia procesal y administrativa para conocer de reclamos en que se invoque la no aplicación o respeto de la Ley 19.628 por los servicios públicos[141].

Si de las facultades del Consejo para la Transparencia no comprenden la protección de datos, y aquello supone que no podría considerarse como una Autoridad de protección de datos, entonces se plantea la necesidad de una reforma legal que implemente una autoridad de protección de datos exclusiva o una autoridad basada en un modelo institucional que, garantice al mismo tiempo el acceso a la información pública y la protección de datos personales.

---

por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta Ley les reconoce" –art. 1–.

[139] Daniel Álvarez Valenzuela, "Acceso a la Información Pública y Protección de Datos Personales. ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos?", *Revista de Derecho: Universidad Católica del Norte*, Nro. 1 (2016), 51-79.

[140] La Ley 20285 señala: "Créase el Consejo para la Transparencia, como una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio (…) Velar por el adecuado cumplimiento de la Ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado" –art. 31.m)–.

[141] Renato Jijena Leiva, "Tratamiento de Datos Personales en el Estado y acceso a la información pública", 89.

En todo caso, advertimos que:

> Hemos analizado desde hace años la necesidad de definir un modelo institucional que garantice al mismo tiempo el acceso a la información administrativa y la protección de datos personales, defendiendo la conveniencia de que fueran las Autoridades de protección de datos también las que actuaran como autoridad independiente de garantía del derecho de acceso a la información pública (…) El modelo de una sola autoridad garante para la protección de datos personales y para el acceso a la información pública está presente en países como Reino Unido o Alemania, aporta seguridad jurídica y facilita una interpretación armónica e integrada de dos derechos que pueden entrar en conflicto[142].

Es preciso mencionar que en 2017 se presentó un Proyecto de Ley –modificatorio a la Ley 19.628– que regula la protección y el tratamiento de los datos. Así también crea la Agencia de Protección de Datos Personales, como una autoridad de control encargada de velar por la protección de los derechos y libertades de las personas titulares de datos y por el adecuado cumplimiento de las normas relativas al tratamiento de estos[143].

Ahora bien, respecto a este derecho fundamental, la Resolución 61146 de la Corte de Apelaciones de Temuco ha precisado que:

> La doctrina y la jurisprudencia comparadas han establecido la existencia de un nuevo derecho fundamental denominado "a la autodeterminación informativa", el que se encuentra implícito en el derecho fundamental a la vida privada (…) De este modo, el derecho a la autodeterminación informativa consiste en la facultad que tiene una persona de ejercer control sobre sus documentos, información o datos personales que se encuentren en registros o bancos de datos públicos o privados.

Asimismo, sobre el *habeas data*, la Resolución 1849-10 de la Corte de Apelaciones de Santiago, expone que:

> La Ley Nº 19.628, sobre Protección de la Vida Privada, define los datos personales como aquellos *"relativos a cualquier información concerniente a personas naturales, identificadas o identificables"* (artículo 2°, letra f) (…) Ello se traduce en el control de las personas sobre sus datos y comprende el derecho a saber sobre la existencia de ficheros o archivos de registro de información de carácter personal, públicos o privados, cuáles son sus finalidades y quiénes son los responsables de los mismos, de manera que las personas concernidas puedan conocer los datos propios contenidos en dichos archivos o ficheros, teniendo el

[142] Troncoso, "La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>", 1052-1053.

[143] El proyecto también busca consagrar un modelo de coordinación regulatoria entre esta autoridad y el Consejo para la Transparencia. El proyecto se encuentra en la etapa de primer trámite constitucional ante el Senado. Las referencias al proyecto e informes de la propuesta pueden consultarse en la siguiente dirección: http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07.

> derecho a actualizarlos o a solicitar mediante el recurso de *habeas data* su rectificación o cancelación.

Puede considerarse el caso chileno como uno de los ordenamientos que más ha avanzado en los últimos años, en su afán de consolidar un sistema jurídico acorde a las necesidades que plantea el derecho a la protección de datos personales. Se evidencia, tanto de la última reforma constitucional que reconoce el derecho fundamental a la protección de datos, como de su regulación, por medio de la Ley 19.628 sobre protección de la vida privada. Además, de los proyectos de reforma de la Ley 19.628 que buscan acreditar a la Agencia de Protección de Datos como una autoridad de control independiente, bajo un modelo de coordinación regulatoria con el Consejo para la Transparencia.

## 2.2 Especial referencia a la situación de Argentina, Uruguay y México

El intento de aproximar a Latinoamérica al modelo europeo en materia de protección de datos personales, en la actualidad empieza a cristalizarse[144]. Siendo el derecho a la protección de datos un derecho global, la ausencia de un modelo homogéneo, no sólo limitaría las relaciones económicas y comerciales sino, además, acrecentaría en "diferencias conceptuales entre los diversos sistemas de derechos humanos, cuya característica fundamental debiera residir precisamente en su universalidad"[145]. Así, la importancia de contar con un marco jurídico apropiado y acorde a estándares internacionales "abre la posibilidad de que los países iberoamericanos se conviertan en un espacio donde sean posibles inversiones y actividades empresariales que impliquen transferencias de datos personales, convirtiendo esa región en un espacio más competitivo para el ámbito de las TIC"[146].

[144] Incluso, como señala Carlos Gregorio en su estudio sobre "Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina" se debería seguir en Latinoamérica la política adoptada por la Unión Europea, es decir: "evitar los inconvenientes de muchas Leyes nacionales de Protección de Datos Personales y lograr una norma común".

[145] Maqueo Ramírez, Moreno y Recio Gayo, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", 93.

[146] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 182.

Desde ya han surgido algunas precisiones sobre este proceso de transformación que son necesarias, en virtud de la evidente dispersión normativa y diferentes tópicos jurídicos, con los que se aborda la regulación del derecho fundamental a la protección de datos en Latinoamérica. Son tres países –Argentina, Uruguay y México– que en el marco latinoamericano merecen una discusión especial, tomando en cuenta el ordenamiento jurídico que han desarrollado y los reconocimientos que desde el ámbito internacional han recibido.

En la región han sido declarados por la Comisión Europea, únicamente, Argentina en 2003 y Uruguay en 2012 como países con un nivel de protección adecuado, a partir del cumplimiento de los estándares que exige la comunidad internacional. Por ejemplo, destacamos que "el marco de protección de estos países estima el reconocimiento de principios; derechos; la existencia de una autoridad de control independiente; y transferencias internaciones de datos amparados en un marco jurídico apropiado que establece el respeto de los datos personales tanto en el ámbito local como internacional"[147].

En el marco europeo el Grupo de Trabajo del artículo 29 –creado por la Directiva 95/46 C/E–, ha desarrollado una actividad importante en relación a los dictámenes sobre el nivel adecuado de protección de datos en países terceros, que se encuentran fuera de la jurisdicción de la Unión Europea. Así, para considerar que un país tiene un nivel adecuado de protección se evalúa, en particular: a) país de origen; b) orden jurídico general o sectorial vigente; c) normas profesionales y medidas de seguridad vigentes[148]. En todo caso, aclaramos que la Directiva 95/46

[147] Cfr. Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 182. Asimismo, señalamos que "en el caso concreto de Argentina y Uruguay, es admisible decir que la Comisión Europea les ha otorgado el reconocimiento como países que efectivamente establecen un nivel adecuado de protección de datos personales, lo que incluso ha llevado a Uruguay a ser el primer y único país en Latinoamérica en haber procedido a la adhesión al Convenio 108 y su Protocolo Adicional, mismos que tienen por objeto establecer las reglas generales para garantizar el respeto a la vida privada (por lo que se refiere al tratamiento automatizado de datos de carácter personal) y simultáneamente la libre circulación de la información". Cfr. Maqueo Ramírez, Moreno y Recio Gayo, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", 93.

[148] En el marco de la transferencia internacional de datos personales, el Grupo de Trabajo del artículo 29, creado por la Directiva 95/46 C/E, constituyó un órgano de carácter consultivo e independiente

ha sido derogada por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo –en adelante RGPD–, lo que conllevará un cambio progresivo y sistemático de la normativa en Europa y, desde luego, en países terceros[149].

En lo relativo a la adecuación de los países, el RGPD señala que la Comisión considerará "de qué manera respeta un determinado tercer país el Estado de Derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos y su Derecho general y sectorial"[150]. Se destaca, además, la evaluación de "garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos"; y finalmente, la existencia de un "control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas" –Considerando 104–.

Si bien en el contexto latinoamericano, hasta ahora el reconocimiento de países con nivel de protección adecuado lo han obtenido Argentina y Uruguay, subrayamos que existe una fuerte tendencia en adoptar el modelo de regulación que exige la Unión Europea. Así, como resultado de los compromisos internacionales que se incluyen en los convenios de cooperación económica, se pone de manifiesto la necesidad de

---

conformado por las autoridades de control designadas por los Estados Miembros de la Unión Europea y que, entre otras atribuciones, garantiza el cumplimiento de la normativa para la protección de datos personales por países terceros a partir de actividades de comercio internacional. Cfr. Agencia Española de Protección de Datos. Disponible en: http://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php.

[149] En cuanto al Grupo de Trabajo del artículo 29, el RGPD señala que toda referencia a éste se entenderá hecha al Comité Europeo de Protección de Datos –art. 94.2–. Asimismo, el RGPD precisa que: "A fin de fomentar la aplicación coherente del presente Reglamento, el Comité debe constituirse como organismo independiente de la Unión. Para cumplir sus objetivos, el Comité debe tener personalidad jurídica. Su presidente debe ostentar su representación. El Comité debe sustituir al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por la Directiva 95/46/CE" –Considerando 139–.

[150] Conforme al RGPD, la evaluación del marco jurídico interno de un tercer país incluye "la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal" –Considerando 104–.

eliminar “obstáculos importantes para el flujo de información, a veces tan necesario para el intercambio comercial y la cooperación internacional”[151].

En este sentido, advertimos que:

> La protección de datos personales, si es importante dentro de la Unión Europea, lo es aún más en un mundo globalizado e interconectado. No nos referimos únicamente al intercambio transfronterizo de datos derivado del incremento de las relaciones personales y comerciales con otros países, especialmente del área Asia-Pacífico. Los tratamientos de datos personales de la propia esfera personal o doméstica que llevan a cabo las redes sociales virtuales –*Facebook, MySpace*– o los motores de búsqueda –de la que la polémica relativa a *Google Street View* es un buen ejemplo– o la prestación de servicios de computación en nube –*Cloud Computing*– implican la existencia de constantes flujos transfronterizos de información personal para los que no siempre ha sido efectiva la normativa europea de protección de datos –y mucho menos la legislación estrictamente nacional–. Estos tratamientos de datos personales se desarrollan por Internet a través de redes internacionales cuyos usuarios y proveedores de servicios se encuentran ubicados en países diferentes y donde el servidor informático se encuentra también en un tercer país[152].

Por ello, tomando en cuenta que la protección de datos es un derecho fundamental que en el contexto global plantea la construcción de un sistema homogéneo, es imprescindible que la comunidad internacional asegure su garantía, mediante estándares comunes que respeten los derechos humanos y la dignidad de la persona, tanto en el ámbito del derecho general como sectorial.

Ahora bien, respecto a la situación de México es oportuno apuntar que su legislación ha desarrollado niveles adecuados de tutela respecto al derecho a la protección de datos. Aunque no ha sido calificado como país con nivel de protección adecuado, cuenta con el reconocimiento internacional de la autoridad de protección de datos, dado por la “Conferencia Internacional de Comisionados de Protección de Datos y Privacidad”[153]. En todo caso –al igual que Uruguay en 2013 y Argentina en 2019–, México se ha adherido, desde el 2018, al Convenio 108 del Consejo de Europa, lo cual representa un avance significativo para alcanzar el equilibrio y la armonía de la legislación de protección de datos en la región.

---

[151] Cfr. Maqueo Ramírez, Moreno y Recio Gayo, “Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario”, 78.
[152] Troncoso, “El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional”.
[153] Cfr. International Conference of Data Protection and Privacy Commissioners. Disponible en: https://privacyconference2019.info/accredited-members-and-observers-2/.

El marco normativo de los países que se señalan en este apartado intenta procurar la tutela de la información personal, mediante el aseguramiento de mecanismos de protección que garantice el control y supervisión, sobre el tratamiento de la información personal. En la búsqueda de un esquema de protección homogéneo, diríamos que –como sucedió en la Unión Europea– estos modelos jurídicos obligan a los Estados latinoamericanos a "adecuar su legislación doméstica al más alto nivel normativo y a adoptar los criterios que determinan su interpretación y alcance"[154].

Por ello, con el fin de homogeneizar criterios es significativo resaltar la actividad que han desarrollado estos países, por cuanto, como advierte la doctrina y la OEA, las tendencias a marcar diferentes modelos de regulación "muchas veces pueden llevar, desde lo literal, a amputaciones innecesarias del instituto, el que debe ser regulado –constitucionalmente y legalmente hablando– de una manera simple y abierta, de forma tal que permita la adecuación a las más variadas posibilidades"[155].

Tomando en cuenta que "la recolección, el almacenamiento, el uso, la circulación y demás actividades sobre los datos personales han sido objeto de una labor de armonización internacional en regulación con miras a lograr un consenso jurídico coherente sobre temas cardinales de dicha materia"[156]; lo que pretendemos, en esta parte es resaltar la necesidad de que los ordenamientos jurídicos sobre protección de datos se equilibren en el ámbito internacional y que el tratamiento de la información personal esté rodeado de garantías mínimas, atendiendo el desarrollo de las tecnologías y la economía digital.

[154] Maqueo Ramírez, Moreno y Recio Gayo, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", 92.
[155] Oscar Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de *habeas data* a dos décadas de su creación", en Eduardo Ferrer y Arturo Zaldívar (coord.), *La Ciencia del Derecho Procesal Constitucional: Procesos Constitucionales de la Libertad*, (México, Instituto de Investigaciones Jurídicas, 2008), 895.
[156] Nelson Remolina y Luisa Álvarez Zuluaga, *Guía GECTI para la implementación del principio de responsabilidad demostrada –accountability- en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos*, (Bogotá: Facultad de Derecho – GECTI, 2018), 11.

### **2.2.1** Argentina

Reconocido como el primer país en la región en contar con la acreditación internacional por la Unión Europea[157], la Constitución de 1994 admite a la acción de amparo como una garantía de protección de la información de carácter personal y del ejercicio de los derechos de supresión, rectificación, confidencialidad o actualización –art. 43–[158]. En este marco, apuntamos que:

> Si bien el país dispone de una normativa sobre protección de datos comprensiva, cuyas disposiciones sustantivas siguen muy de cerca los estándares de la Unión Europea, no sucede lo mismo con los mecanismos previstos para garantizar su cumplimiento (…) la ley aún requiere la implementación de sus disposiciones, en lo concerniente a mecanismos de protección, en un significativo número de las provincias, esto es, la protección es aún fragmentaria[159].

Esta protección fragmentaria es evidente, por cuanto la Constitución de la provincia de Buenos Aires, propiamente, desarrolla y reconoce la garantía del *habeas data* –art. 20.3–[160]. En todo caso, la promulgación de la Ley 25.326 de datos personales constituyó un significativo precedente para el desarrollo del mandato constitucional contemplado en el art. 43, y por el cual se garantizaría la protección de los datos personales[161]. En la era de la información y de los datos, la importancia de una Ley

---

[157] Véase la Decisión de la Comisión en: https://tinyurl.com/rpu8exm

[158] En este ámbito, la Constitución reconoce que: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos" –art.43–.

[159] Alberto Cerda Silva, "El nivel adecuado de protección para las transferencias internacionales de datos personales desde la Unión Europea", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, Nro. 1 (2011), 327 – 356.

[160] La Constitución de la provincia de Buenos Aires determina que: "A través de la garantía de *Habeas data*, que se regirá por el procedimiento que la Ley determine, toda persona podrá conocer lo que conste de la misma en forma de registro, archivo o banco de datos de organismos públicos, o privados destinados a proveer informes, así como la finalidad a que se destine esa información, y a requerir su rectificación, actualización o cancelación. No podrá afectarse el secreto de las fuentes y el contenido de la información periodística. Ningún dato podrá registrarse con fines discriminatorios ni será proporcionado a terceros, salvo que tengan un interés legítimo. El uso de la informática no podrá vulnerar el honor, la intimidad personal y familiar y el pleno ejercicio de los derechos" –art. 20.3–.

[161] La Ley 25.326 señala que: "La presente Ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que

por el estilo se justifica porque "regula a todo aquel que trata datos. Si una persona o entidad recopila datos personales, entonces tiene que cumplir con una serie de obligaciones, desde registrar la base de datos, hasta dar acceso y corrección en caso de que tengan datos erróneos"[162].

Además, siendo el segundo país latinoamericano en contar con una Ley de Protección de Datos, la promulgación de la Ley 25.326 constituyó el antecedente para ser considerado como el primer país de la región en lograr el reconocimiento internacional de país con un nivel adecuado[163]. Sobre esta consideración, varios son los criterios por los cuales se justifica. Por ejemplo, Alberto Cerda sostiene que:

> En general, la ley de Argentina cumple con todos los requerimientos sustantivos que la Unión Europea suele constatar en su examen. De hecho, al analizar la seguridad del país, el Grupo del artículo 29 sobre Protección de Datos constató un satisfactorio nivel de protección en las disposiciones sustantivas, tales como aquellas relativas al ámbito de aplicación, los principios generales aplicables al tratamiento de datos, los derechos del titular de datos personales, y las obligaciones de las entidades responsables de dicho tratamiento[164].

Así también Mario Oryazabal considera que "el legislador argentino siguió en general las pautas de la Directiva Europea 95/46/CE de 1995 (arts. 25 y 26), que refleja la rica experiencia europea de los años 1980-90 en lo que respecta a la protección y a la libre circulación de los datos"[165].

---

sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional" –art. 1–.

[162] Pablo Palazzi, "Periodismo de datos y datos personales: algunas reflexiones sobre la aplicación de la Ley de protección de datos personales a la prensa en la Argentina.", *Revista Latinoamericana de Protección de Datos Personales*, Nro. 3 (2012), ISSN 2422-6769.

[163] Sobre este respecto, destacamos que la Decisión de la Comisión Europea, sobre la adecuación de la protección de los datos personales en Argentina señaló que: "La Ley 25 326 sobre protección de datos personales, de 4 de octubre de 2000 (en lo sucesivo denominada "la Ley") desarrolla y amplía lo dispuesto en la Constitución. Contiene normas sobre los principios generales de protección de datos, los derechos de los titulares de datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial habeas data". Véase la Decisión de la Comisión en: https://tinyurl.com/rpu8exm. A esto, hay que agregar que, en 2019, Argentina se convirtió en el tercer país latinoamericano en adherirse al Convenio 108, con el objeto de proporcionar a su normativa de protección de datos mayor seguridad jurídica.

[164] Cerda Silva, "El nivel adecuado de protección para las transferencias internacionales de datos personales desde la Unión Europea", 343.

[165] Mario Oryazabal, "El Derecho a la Intimidad y el tratamiento de datos personales en el Derecho Internacional Privado Argentino", *Revista de la Facultad de Derecho de la Universidad Nacional de Buenos Aires*, Nro. 83 (2007), 49-78.

Por otra parte, destacamos la Ley 14.214 sobre *habeas data* de la provincia de Buenos Aires, la cual reglamenta el procedimiento constitucional previsto en el art. 43 de la Constitución Nacional y el art. 20.3 de la Constitución de la provincia de Buenos Aires[166]. Y, la promulgación de la Ley Nro. 26951 de 2014, que crea –en el ámbito de la Dirección Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia y Derechos Humanos– el Registro Nacional "No Llame" orientado a regular el tratamiento de la información personal en el entorno de los servicios de telefonía[167].

Encontrándose vigente el RGPD, se propuso, en 2015, ante el Senado de Argentina el Proyecto de Ley sobre "El derecho al Olvido". Con referencia a este aspecto, advertimos que:

> En cuanto a Argentina, no hay normas en la ley 25.326 como las que existen en la directiva (art. 4). Por eso, la determinación de la ley aplicable al tratamiento de datos personales en Internet es difícil de abordar y debe recurrirse a los principios generales del Derecho, o desarrollar nuevos criterios para poder determinar la competencia territorial de las normas locales en Internet (…) En Argentina los tribunales también reconocieron el derecho al olvido en materia de informes comerciales antes de que la ley 25.326 los contemplara en forma expresa. Por ende no parece difícil que el derecho al olvido tenga andamiento jurisprudencial antes de que la ley 25.326 lo recepte en una futura reforma legislativa, aunque se deberá tener en cuenta las limitaciones que la ley 25.326 establece para la prensa y cómo impactan en los buscadores[168].

El interés por mantener un orden jurídico de protección de datos acorde a escenarios internacionales ha precisado la formulación de este tipo de normas que se consideran, en suma, como una de las novedades dentro del RGPD[169]. Sobre esta cuestión, uno de los antecedentes más relevantes en el ámbito internacional,

---

[166] El objeto de la Ley 14.214 se enmarca en "la reglamentación del proceso constitucional de *habeas data*, de conformidad a lo establecido en el artículo 20º inciso 3) de la Constitución" –art. 1–.

[167] Así también el objeto de la Ley 26.951 determina: "proteger a los titulares o usuarios autorizados de los servicios de telefonía, en cualquiera de sus modalidades, de los abusos del procedimiento de contacto, publicidad, oferta, venta y regalo de bienes o servicios no solicitados" –art. 1–.

[168] Pablo Palazzi, "El reconocimiento en Europa del derecho al olvido en Internet", *Revista Jurídica: La Justicia Uruguaya,* Nro. 150 (2014). ISSN 0797-2695. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=5743527.

[169] Precisamente, el RGPD señala que:" A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos" –Considerando 66–.

es el caso Costeja Vs Google en donde el Tribunal de Justicia de la Unión Europea respaldó el derecho al olvido en Internet, garantizando la protección de datos y la privacidad de las personas[170]. Desde esta perspectiva, entendemos que "los ciudadanos cada vez son más conscientes de ello y quieren poder controlar la información que sobre ellos circula por Internet. Y una forma de este control es la petición de su borrado y no indexación"[171]. El derecho al olvido "ha cobrado especial relevancia frente a publicaciones en internet de hechos verdaderos del pasado de las personas, que ahora, por motivos particulares de los afectados, desean que se suprima definitivamente"[172]. Por ello, se reconoce la necesidad de introducir urgentes reformas a la Ley 25.326, por cuanto "responde al marco jurídico vigente en tiempos en que ni siquiera existía Internet del modo que lo concebimos hoy y que decididamente no atiende a ni a los principales fenómenos derivados del actual grado de desarrollo de las tecnologías"[173].

Ahora bien, el antecedente más considerable para el desarrollo del derecho a la protección de datos lo encontramos en la jurisprudencia de la Corte Suprema de Justicia de la Nación. Así, sobre el reconocimiento de este derecho, la Sentencia XXXlll del 15 de octubre de 1998 precisa que:

> La protección legal se dirige a que el particular interesado tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga. En tal sentido, este derecho forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad. El señorío del hombre sobre sí se extiende a los datos sobre sus hábitos y costumbres, su sistema de valores y de creencias, su patrimonio, sus relaciones familiares, económicas y sociales, respecto de todo lo cual tiene derecho a la autodeterminación informativa.

Asimismo, sobre el derecho de las personas para promover una acción constitucional para la protección de datos personales, esta Resolución apunta que:

---

[170] Véase la Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014. Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González. Disponible en: https://tinyurl.com/wsr6wgh.

[171] Mónica Arenas Ramiro, "*Unforgettable*: A propósito de la STJUE de 13 de mayo de 2014. Caso Costeja (*Google* Vs. AEPD)", *Revista Teoría y Realidad Constitucional*, Nro. 34 (2014):537-558.

[172] Nelson Remolina, "¿Derecho al olvido en el ciberespacio? Principios internacionales y reflexiones sobre las regulaciones latinoamericanas", en Agustina Del Campo (coord.), *Hacia una Internet libre de censura II: Perspectivas en América Latina*, (Buenos Aires, Universidad de Palermo, 2017), 224.

[173] Oscar Puccinelli, "Un proyecto de reforma a la Ley 25.326 que está a la altura de las Leyes más avanzadas del mundo", *Revista Latinoamericana de Protección de Datos Personales*, Nro. 4 (2017). Disponible en: https://tinyurl.com/v3mgvrs.

> A esta decisión se le atribuye la configuración del concepto de "autodeterminación informativa" o libertad informática, que es reconocido actualmente en forma predominante como el fundamento del *habeas data* en las legislaciones que contemplan derechos análogos (…) Según este concepto es el ciudadano quien debe decidir sobre la cesión y uso de sus datos personales. Este derecho -se dijo- puede ser restringido por medio de una ley por razones de utilidad social, pero respetando el principio de proporcionalidad y garantizando que no se produzca la vulneración del derecho a la personalidad.

En relación a la autoridad de protección de datos personales –a partir de lo dispuesto por el Decreto Nro. 1558/2001–, se designó a la Dirección Nacional de Protección de Datos Personales (DNPDP) como el órgano de control de las disposiciones contenidas en la Ley 25.326[174]. En este caso, consideramos que:

> La ley argentina ha suscitado varias cuestiones en torno a su efectivo cumplimiento. En particular, de acuerdo al reporte elaborado por el Grupo del artículo 29 sobre Protección de Datos, hay tres dificultades asociadas con su cumplimiento: la ausencia de una autoridad de protección de datos independiente, la necesidad de crear agencias de control, y la urgencia de implementar la normativa sobre medidas judiciales a nivel de las provincias. La autoridad sobre protección de datos de la Argentina no es independiente. Inicialmente, la propuesta de ley que devino en la ley de protección de datos establecía una autoridad con "autonomía funcional", pero ello fue eliminado a través de veto presidencial, por razones presupuestarias. Más tarde, nuevamente a través de un decreto presidencial, la DNPDP fue creada, como un servicio público dependiente del Ministerio de Justicia y Derechos Humanos[175].

En todo caso, no existe un consenso para afirmar que la máxima autoridad de protección de datos personales tenga la suficiente independencia como una autoridad de control. Los cuestionamientos se fundamentan en la asignación presupuestaria que depende de otra jerarquía. Es importante señalar que, mediante el Decreto Nro. 746/2017, las atribuciones conferidas a la DNPDP –en calidad de autoridad de control para la aplicación de la Ley 25.326– se han delegado a la Agencia de Acceso a la Información Pública, cuya misión se orienta a garantizar el ejercicio del derecho de acceso a la información pública y a la protección de los datos[176]. En sus actividades de control, ha desarrollado un Registro Nacional de

[174] El Decreto Nro. 1558/2001 dispuso: "Créase la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, en el ámbito de la SECRETARIA DE JUSTICIA Y ASUNTOS LEGISLATIVOS del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, como órgano de control de la Ley Nº 25.326. El Director tendrá dedicación exclusiva en su función, ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones" –art. 29–.

[175] Cerda Silva, "El nivel adecuado de protección para las transferencias internacionales de datos personales desde la Unión Europea", 344.

[176] Esta delegación, contenida en el Decreto Nro. 746/2017 dispuso que: "Sustitúyese el artículo 19 de la Ley N° 27.275 por el siguiente: "ARTÍCULO 19.- AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA. Créase la AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA, como ente autárquico que funcionará con autonomía funcional en el ámbito de la JEFATURA DE GABINETE DE

Documentos y un Centro de Asistencia a las Víctimas de Robo de Identidad; contribuido con campañas de cultura sobre privacidad y protección de los datos, a través de asesoramiento a los titulares de la información y consulta web del Repertorio de Jurisprudencia sobre *habeas data*. Y así también ha elaborado dictámenes sobre protección de datos, los cuales han surgido como resultado de las denuncias y reclamos.

Esta autoridad de protección datos ha desempeñado un papel relevante en su objetivo de concretar el control y supervisión de este derecho fundamental. Así, lo reconoció en 2014 el "*Berkman Klein Center for Internet & Society*" de la Universidad de Harvard, en virtud del Programa "Con Vos en la Web" para la protección de datos de niños, niñas y adolescentes en Internet, considerándola como una propuesta de política pública exitosa de la región. A esto, se suma que en noviembre de 2016 fue nombrada como miembro del Comité Ejecutivo de la RIPD, junto con las autoridades de protección de datos de Colombia y México.

Más allá de la discusión vinculada con la falta de autonomía presupuestaria, la labor desarrollada como un organismo de control ha permitido demostrar un nivel adecuado de protección[177]. Sus funciones se encuentran enmarcadas en conocer y controlar la efectiva protección de los datos personales y, además, asesorar a los

MINISTROS. La AGENCIA DE ACCESO A LA INFORMACIÓN PÚBLICA debe velar por el cumplimiento de los principios y procedimientos establecidos en la presente Ley, garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover medidas de transparencia activa y actuar como Autoridad de Aplicación de la Ley de Protección de Datos Personales N° 25.326". Cabe señalar que la referencia realizada a la Ley N° 27.275 refiere a la Ley que regula el Derecho de Acceso a la Información Pública. En materia de protección de datos personales, la Ley N° 27.275 (art. 8.i) refiere que podrá exceptuarse de proveer la información cuando se trate de: "Información que contenga datos personales y no pueda brindarse aplicando procedimientos de disociación, salvo que se cumpla con las condiciones de licitud previstas en la Ley 25.326 de protección de datos personales y sus modificatorias" –art. 11–.

[177] Sobre la independencia de las autoridades de control, la jurisprudencia del TJUE anota que las autoridades "tienen que actuar con objetividad e imparcialidad. Por tanto, «han de disfrutar de la independencia que les permita ejercer sus funciones sin influencia externa». «Esta independencia excluye no sólo cualquier influencia que pudieran ejercer los organismos sujetos a control sino también toda orden o influencia externa con independencia de la forma que revista, directa o indirecta, que pudiera orientar sus decisiones y, en consecuencia, poner en peligro el cumplimiento de la tarea que corresponde a dichas autoridades de establecer un justo equilibrio entre la protección del derecho a la intimidad y la libre circulación de datos personales»". Cfr. SSTJUE, de 9 de marzo de 2010 —apdo. 19, 25, 30 y 50—, de 16 de octubre de 2012 —apdo. 41-43— y de 8 de abril de 2014 —apdo. 51—.

titulares de datos personales sobre las injerencias que pueden afectar a su información, asegurando su desarrollo, por medio de la recepción de denuncias.

### **2.2.2** Uruguay

La Constitución materializa el reconocimiento del derecho a la protección de datos, por medio de las libertades fundamentales relacionadas con el derecho a la intimidad, a la inviolabilidad de la correspondencia y a la dignidad de las personas[178]. Si bien no existe un reconocimiento –como un derecho autónomo– de la protección de datos personales y del *habeas data*, apreciamos que:

> La Constitución uruguaya no reconoce expresamente la acción de *habeas data*, pero para cierta doctrina encuentra un fundamento similar al amparo y surge de la interpretación lógico-sistemática-teleológica de los artículos 7º., 10, 28, 72 y 332, de los cuales surge de manera indudable el derecho de todo habitante a conocer la información que sobre él se posea, el derecho a solicitar la rectificación de datos erróneos y la supresión de los datos sensibles[179].

Con fundamento en el mandato constitucional previsto en el art. 72, por el cual los derechos, deberes y garantías no excluye otros que son inherentes a la persona humana, la Ley Nro. 18331 de Protección de Datos reconoce a la protección de datos personales como un derecho fundamental inherente a la persona humana[180] y garantiza su tutela, por medio del *habeas data*[181]. De esta manera, consideramos

---

[178] Sobre este reconocimiento, la Constitución determina que: "Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad" –art. 7 –; "El hogar es un sagrado inviolable" –art. 11–; "Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables" –art. 28–; "La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno" –art. 72–; "Los preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de la reglamentación respectiva, sino que ésta será suplida, recurriendo a los fundamentos de Leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas" –art. 332–.

[179] Oscar Puccinelli, "Apuntes sobre el derecho, la acción y el proceso de *habeas data* a dos décadas de su creación", 863.

[180] La Ley Nro. 18331 enmarca su objeto en la "aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado" –art. 3–.

[181] Así también dicha Ley reconoce que: "Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y -en caso de error, falsedad, prohibición de

que esta normativa "adopta el modelo europeo estatuyendo un conjunto de principios tuitivos generales, una serie de derechos de los titulares de los datos, regímenes particulares para segmentos de datos calificados como especialmente protegidos, y un régimen de registro de bases de datos personales"[182].

Como hemos precisado, este marco general de protección obtuvo el reconocimiento internacional como país con nivel adecuado de protección por la Unión Europea[183]. Posterior a este reconocimiento, mediante la Ley Nro. 19.030 se suscribió y aprobó el Convenio N°108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, así como también su Protocolo Adicional, convirtiéndose, de esta manera, en el primer país latinoamericano en adherirse a dicho convenio. En este sentido, apuntamos que:

> La finalidad del Tratado al que Uruguay se adhiere, es garantizar, en el territorio de cada Parte, a toda persona física, el respeto de sus derechos y libertades fundamentales, independientemente de su nacionalidad o su residencia. Más concretamente, se alude al derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona, lo que el propio texto aprobado califica como «protección de datos»[184].

Por otra parte, la Ley Nro. 18331 dispuso la creación de la Unidad Reguladora y de Control de Datos Personales (URCDP), a través de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento. Se crea un órgano de regulación y control "con autonomía técnica y competencias suficientes como para contribuir a la capilaridad e inserción efectivas

tratamiento, discriminación o desactualización- a exigir su rectificación, inclusión, supresión o lo que entienda corresponder" –art. 37–.

[182] Marcelo Bauzá, "Derechos Fundamentales", en *Privacidad y Tecnología en equilibrio*, (Uruguay: Unidad Reguladora y de Control de Datos Personales, 2012), 16-17.

[183] La Decisión de la Comisión Europea sobre la adecuación de la protección de los datos personales en Uruguay señaló que "las normas jurídicas de protección de datos aplicables en la República Oriental del Uruguay cumplen todos los principios básicos necesarios para ofrecer un nivel adecuado de protección a las personas físicas, y también prevén excepciones y limitaciones para proteger intereses públicos importantes. Estas normas jurídicas de protección de datos y excepciones se basan en los principios establecidos en la Directiva 95/46/CE". Véase la Decisión de la Comisión en: https://tinyurl.com/v4stsdp.

[184] Marcelo Bauzá, "Derechos Fundamentales", 18.

del régimen en los diversos estratos de la sociedad (incluyendo potestades sancionatorias administrativas)"[185].

La actividad de la URCDP –enmarcada en vigilar el cumplimiento de la normativa aplicable al derecho a la protección de datos personales– llevó a que en 2016 fuera designada para ejercer la Presidencia de la RIPD. La crítica sobre esta autoridad de control también podría extenderse sobre el carácter independiente como una autoridad de protección de datos, por cuanto el Consejo que la preside se integra por dos miembros designados por el Poder Ejecutivo. No obstante, a partir del reconocimiento como país con nivel adecuado, se considera que la URCDP actúa con absoluta independencia[186]. Las disposiciones de la Ley Nro. 18331 hace que la URCDP se configure como una autoridad con amplia autonomía técnica y jurídica que dicta resoluciones, dictámenes y elabora informes para la observancia del derecho a la protección de datos[187]. Se compone de un Consejo Ejecutivo y Consultivo; ejecuta programas de promoción y participación ciudadana como "Tus derechos Valen. Cuídalos", con el fin de concientizar sobre las implicaciones tecnológicas y culturales que se desprenden de este derecho fundamental.

Finalmente, la jurisprudencia del Tribunal de Apelaciones, en la Sentencia 12 de 2008, destaca que el *habeas data*:

> Constituye un proceso principal y el natural para el objeto planteado, porque actualmente el procedimiento previsto por los arts. 37 a 45 de la Ley N° 18.331 de 11/8/2008 es el común que el ordenamiento jurídico prevé para las pretensiones que tengan por objeto exclusivo el

[185] Ibíd., 17.

[186] La Decisión de la Comisión Europea destaca que "la aplicación de las normas jurídicas de protección de datos está garantizada por recursos judiciales y administrativos y, en particular, por la acción Habeas Data, que permite al interesado emprender una acción judicial contra el responsable del tratamiento de datos para ejercitar su derecho de acceso, rectificación y supresión, así como por el control independiente que realiza la autoridad de control, la Unidad Reguladora y de Control de Datos Personales (URCDP), que tiene facultades de investigación, intervención y sanción, en consonancia con el artículo 28 de la Directiva 95/46/CE, y actúa con absoluta independencia. Además, cualquier parte interesada puede interponer un recurso para solicitar una indemnización por daños y perjuicios causados por un tratamiento ilegal de los datos personales". Véase la Decisión de la Comisión en: https://tinyurl.com/v4stsdp.

[187] Durante el 2015 se analizaron los expedientes presentados ante la URCDP, en donde se constató la expedición de 129 resoluciones y 21 dictámenes. En función de los requerimientos que ha recibido la URCDP se han elaborado 331 informes, que incluyen los puntos de vista jurídico, notarial y técnico. Cfr. Unidad Reguladora y de Control de Datos Personales. "Memoria Anual de la Unidad Reguladora y de Control de Datos Personales", 2015. Disponible de: https://tinyurl.com/ukrckb6.

> *habeas data*, o sea, el acceso a la información en bases de datos, su rectificación, inclusión o supresión.

Así también, en relación a la naturaleza del derecho a la protección de datos, la Sentencia 4 de 2015 del Tribunal de Apelaciones advierte que:

> Hubiera sido preferible que la actora citara también, expresamente y no de modo tangencial o implícito en su exposición, el derecho a la seguridad en la protección de datos personales, a la intimidad, inviolabilidad de las comunicaciones y exclusión de las acciones privadas del quehacer estatal cuando no afectan el ordenamiento jurídico, garantizados por los artículos 7 y 10 de la Constitución para todo habitante de la República y esenciales en un Estado de Derecho sometido al régimen democrático-republicano de gobierno.

El ordenamiento jurídico de este país representa uno de los esquemas de regulación más importantes de la región. Por ello, advertimos que "la legislación uruguaya, posterior a la argentina, es, posiblemente, más garantista que ésta última"[188]. No obstante, la entrada en vigencia del RGPD también supone que este marco normativo debe impulsar reformas relacionadas con: el ámbito territorial de aplicación, los procedimientos de vulneraciones de seguridad, la ampliación del alcance del principio de responsabilidad, la responsabilidad y contratación de servicios de terceros y la designación de un Delegado de Protección de Datos[189].

### **2.2.3** México

El marco jurídico mexicano es considerado como uno de los más importantes en el contexto latinoamericano. La Constitución protege el derecho a la intimidad de la vida privada –art. 6–, y garantiza a todas las personas el derecho a la protección de sus datos personales, así como también el derecho al acceso, a la rectificación y a la cancelación de los datos –art. 16–. En este contexto, destacamos que:

> Incluso antes de la reforma del artículo 6 constitucional y de la propuesta de reforma al 16, se venían haciendo esfuerzos muy loables en torno al derecho a la protección de datos personales; no obstante, la dimensión de este derecho seguía sin tener la profundidad requerida para dotar al gobernado de una herramienta efectiva que le permitiera equilibrar

[188] Troncoso, "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional".
[189] Cfr. Ana Brian Nougreres, "El sistema uruguayo de protección de datos personales y su posicionamiento global", *Revista Latinoamericana de Protección de Datos Personales*, Nro. 5 (2018). Disponible en: https://tinyurl.com/uj7kyf2.

> su situación jurídica frente al vertiginoso desarrollo tecnológico y al puntaje por comercio internacional que al mismo acompaña[190].

La protección de este derecho fundamental se ha consolidado, tanto en lo conceptual y procesal como en lo institucional. En lo conceptual, la Constitución reconoce a la protección de datos como un derecho autónomo, lo cual incluye la protección del derecho a la intimidad de la vida privada[191]. En este aspecto, apuntamos que:

> Son diversos los rasgos que adquirió el derecho a la protección de datos personales tras haber sido dotado con el carácter de derecho fundamental, de los que destacamos tres: su relación con los demás derechos humanos, su establecimiento como principio o norma de valor, y la obligación de los poderes públicos, en especial del aparato legislativo, de respetar su contenido esencial en caso de una posible intervención[192].

En lo procesal se garantiza el derecho al acceso, a la rectificación y a la cancelación de los datos personales[193], permitiendo al titular de la información ejercer estas facultades como un mecanismo de control, frente al tratamiento de la información personal. Esto es lo que conocemos como la garantía del *habeas data*, por la cual, "debido a las facultades otorgadas a las personas y a los mecanismos de acceso,

---

[190] Lina Ornellas Núñez y Sergio López Ayllón, "La recepción del derecho a la protección de datos en México: Breve descripción de su origen y status legislativo", en Instituto Federal de Acceso a la Información Pública, "*Compendio de lecturas y legislación: Protección de Datos Personales"*, (México: Instituto Federal de Acceso a la Información Pública, 2010), 67.

[191] La Constitución reconoce que: "II. La información referente a la intimidad de la vida privada y la imagen de las personas será protegida a través de un marco jurídico rígido de tratamiento y manejo de datos personales, con las excepciones que establezca la Ley reglamentaria" –art. 6–. Asimismo, garantiza que: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la Ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros" –art. 16–.

[192] Víctor Hugo Hiram, "Derecho a la protección de datos personales. Su diseño constitucional", *Revista de Estudios en Derecho a la Información*, Nro. 2 (2016), 25-45.

[193] La Constitución determina que: "III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de estos; V. Los procedimientos de acceso a la información pública, de acceso, corrección y supresión de datos personales, así como los recursos de revisión derivados de los mismos, podrán tramitarse por medios electrónicos, a través de un sistema automatizado que para tal efecto establezca la Ley reglamentaria y el organismo autónomo garante en el ámbito de su competencia" –art. 6–.

rectificación, cancelación y oposición, el núcleo duro podría establecerse en la potestad de disposición y manejo de la información"[194].

Finalmente, en lo institucional la garantía de este derecho fundamental se materializa en un organismo autónomo o una autoridad de control, que es la responsable de supervisar el cumplimiento de la legislación sobre protección de datos[195]. Dicha autoridad recae en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Así, la actividad desarrollada por esta autoridad de control:

> En esta materia es de la mayor relevancia ya que puede llegar a constituirse en el factor que, por una parte, permita que el derecho a la protección de datos personales, dentro de los límites de la legalidad, responda a las exigencias a las que la realidad nos enfrenta, y por la otra facilite elementos orientadores que conduzcan al mejor entendimiento y aplicación de la norma jurídica a los casos que se le presenten[196].

Por otra parte, la Ley Federal de Protección de Datos Personales en posesión de particulares –orientada a regular el tratamiento legítimo, controlado e informado de la información personal–[197] fue elaborada bajo una influencia del derecho y jurisprudencia comparada. Por ello, apuntamos que:

> Uno de los principios fundamentales sobre el cual se erige dicha normativa es la «expectativa razonable de privacidad», entendida como la confianza que deposita cualquier persona en otra respecto de que los datos personales proporcionados entre ellos, serán tratados conforme a lo que acordaron las partes en los términos establecidos en las leyes. Dicha acepción proviene del derecho anglosajón (*reasonable expectation of privacy*), específicamente de la jurisprudencia norteamericana. Su utilidad es bastante común de parte

[194] Hiram, "Derecho a la protección de datos personales. Su diseño constitucional", *Revista de Estudios en Derecho a la Información*, Nro. 2 (2016), 42.

[195] El artículo 5 de la Constitución refiere que: "El Estado contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica y de gestión (…) responsable de garantizar el cumplimiento del derecho de transparencia, acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la Ley. El organismo autónomo garante previsto en esta fracción, se regirá por la Ley en materia de transparencia, acceso a la información pública y protección de datos personales en posesión de sujetos obligados".

[196] Ornellas Núñez y López Ayllón, "La recepción del derecho a la protección de datos en México: Breve descripción de su origen y status legislativo", 65.

[197] La Ley Federal de protección de datos personales en posesión de particulares tiene por objeto: "la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas" –art. 1–.

> de los jueces en aquel país, y se emplea con la finalidad de determinar si ha existido alguna violación a la privacidad[198].

Ahora bien, la jurisprudencia ha desarrollado relevantes criterios en la materia. Por ejemplo, la Tesis Jurisprudencial Nro. PC.I.A. J/12 K de los Plenos de Circuito destaca que:

> El derecho a la protección de los datos personales está previsto esencialmente en los artículos 6o. y 16 de la Constitución Política de los Estados Unidos Mexicanos (…) con la finalidad de proteger al titular de la información para que pueda manifestar su oposición a la divulgación, no sólo de sus propios datos personales, sino también de los concernientes a su persona, esto es, los que ponen en riesgo su vida, seguridad o salud, los secretos industriales, fiscales, bancarios, fiduciarios o cualquier otro considerado como tal por una disposición jurídica.

En relación a las características del derecho a la protección de datos, la Sentencia Nro. SUP-RAP-37-2013 de la Sala Superior señala que:

> El derecho a la autodeterminación informativa refiere, como se anticipó, a la prerrogativa que todo individuo tiene frente a cualquier ente público o privado, de que no se inmiscuyan sin autorización expresa de él mismo o por mandato de ley o jurisdiccional, en los señalados aspectos de su personalidad que no son públicos sino que pertenecen a su entorno privado, para conocerlos, conservarlos, procesarlos y/o transmitirlos, independientemente de que dicha acción le pueda causar o no alguna molestia (…) La postura que ha adoptado la Sala Superior en lo relativo al derecho de autodeterminación informativa, ha seguido la orientación de la Corte Interamericana de Derechos Humanos, en el sentido de que una injerencia en el ámbito íntimo de las personas para que sea legal, debe reunir como requisito el estar prevista en la ley en sentido formal y material; perseguir un fin legítimo; y ser idónea, necesaria y proporcional.

Bajo estas consideraciones, la legislación de protección de datos ha logrado afirmar la garantía de este derecho fundamental, incluso, con sustento en las recomendaciones de la Corte Interamericana de Derechos Humanos. Existe una tutela amplia, apegada, además, al modelo europeo, particularmente, el español. Así también habiéndose adherido al Convenio N°108 del Consejo de Europa en 2018, se espera que en los siguientes años reciba el reconocimiento de país adecuado ya que, además, su autoridad de protección de datos (INAI) está

[198] Rogelio López Sánchez y José Leal Espinoza, *El derecho a la información y datos personales en México: una visión comparada con el sistema interamericano y europeo de derechos humanos*, (Madrid: Dykinson, 2018), 107-108.

reconocida por la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad y, en todo caso, forma parte del Comité Ejecutivo de la RIPD[199].

Llegados a este punto, evidenciamos notables diferencias entre los países que han recibido reconocimiento internacional en relación con otros que aún empiezan o se encuentran en proceso de consolidar un modelo adecuado de protección. En este sentido, surgen algunas interrogantes: ¿Es necesario un marco común que regule el derecho fundamental a la protección de datos personales en Latinoamérica? ¿Qué funcionalidad tendrían los principios que ha desarrollado sobre la materia la Organización de los Estados Americanos? La idea en este plano no es extraña. La Unión Europea ha tenido resultados favorables, a partir de un marco regulador común sostenido en Directivas y Reglamentos, destinados a materializar un nivel adecuado. En el contexto latinoamericano habría que dedicar especial atención a la Guía Legislativa propuesta por la OEA y los Estándares de protección de datos personales para los Estados Iberoamericanos. Ambos instrumentos tienen como fin la elaboración de una "Ley Modelo Interamericana sobre protección de datos personales" y promover un esquema de regulación homogéneo y equilibrado que garantice la seguridad jurídica del derecho a la protección de datos.

## 3. Enmarque del derecho fundamental a la protección de datos personales en la Unión Europea. Referencia a su regulación en España

A diferencia de los países latinoamericanos, la evolución del derecho a la protección de datos en la Unión Europea ha tenido mayor desarrollo. En primer término, este derecho fundamental se ha fortalecido, mediante "la actividad del TJCE, «vía pretoriana», como todos los demás derechos fundamentales, pero, también, y especialmente, a través de la actividad normativa de las instituciones, que ha

[199] Cfr. International Conference of Data Protection and Privacy Commissioners. Disponible en: https://privacyconference2019.info/accredited-members-and-observers-2/.

desempeñado un papel determinante en el reconocimiento y desarrollo del derecho y en la labor del TJCE"[200].

En este ámbito territorial, el derecho a la protección de datos se presenta "con un carácter de derecho humano autónomo, aunque interrelacionado con el derecho a la vida privada, cuyo alcance se proyecta tanto en el reconocimiento del derecho a la autodeterminación informativa de las personas, como del habeas data"[201]. Si bien, "es finalmente su reconocimiento en la Carta de Derechos Fundamentales de la Unión Europea lo que le otorga un nuevo status"[202], advertimos, además, que "la evolución jurisprudencial ha reconocido y afirmado este nuevo derecho de libertad en los términos de protección de la autonomía individual, como exigencia pasiva en relación con los detentadores del poder informático, de los particulares o de las autoridades públicas"[203].

A la luz del desarrollo normativo de la Unión Europea, desde 1981, el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal representa el primer instrumento, con el que el Consejo de Europa reconoce los elementos esenciales que configuran este derecho fundamental. Por medio de este Convenio, los Estados miembros del Consejo de Europa "tomaron especialmente en cuenta la intensificación de la circulación a través de las fronteras de los datos personales objeto de tratamientos automatizados y la necesidad de conciliar el respeto a la vida privada y la libre circulación de la información entre los pueblos"[204].

---

[200] Mónica Arenas Ramiro, "La protección de datos personales en los países de la Unión Europea", *Revista Jurídica de Castilla y León*, Nro. 16 (2008):113-168.

[201] Maqueo Ramírez, Moreno y Recio Gayo, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", 93. Corresponde señalar que "la regulación europea sobre el tratamiento de datos personales ha incidido en las normas de los países latinoamericanos a tal punto que en muchas cuestiones las Leyes de los últimos países son iguales o similares a lo que establecen las disposiciones europeas". Cfr. Nelson Remolina, "¿Derecho al olvido en el ciberespacio? Principios internacionales y reflexiones sobre las regulaciones latinoamericanas", 216.

[202] Arenas Ramiro, "La protección de datos personales en los países de la Unión Europea", 121.

[203] Frosini, "Nuevas tecnologías y constitucionalismo", 31.

[204] Artemi Rallo Lombarte, "El nuevo derecho a la protección de datos", *Revista Española de Derecho Constitucional*, Nro. 116 (2019), 45-74.

Así, existiendo desde aquella época la necesidad de "resolver la tensión existente entre el uso cada vez más generalizado de la informática y el riesgo que el mismo puede suponer para la vida privada. Informática *versus* intimidad"[205]; el Convenio 108 y su Protocolo Adicional constituyó "el documento base para la discusión de una norma internacional para la protección de datos personales"[206]. Por tanto, en el ámbito comunitario el Convenio 108 del Consejo de Europa representa un documento base. Significa para la protección de datos personales "los principios sobre los que descansará el régimen jurídico del derecho, después reconocido como derecho fundamental"[207]. Sumado a otros instrumentos comunitarios, el cumplimiento del Convenio 108 ha caracterizado que en los Estados de la Unión Europea la regulación se concrete "por el alto grado de homogeneidad entre las normas existentes sobre la materia"[208].

Varios factores contribuyeron para que la protección de la información personal se considere como un derecho nuevo y, naturalmente, autónomo del derecho a la intimidad. Aportes que como anotamos "no son otros que los vinculados a una suerte de diálogo entre la doctrina, los legisladores internacional, comunitario y estatal y la jurisprudencia"[209].

> Buena muestra de la importancia del derecho fundamental a la protección de datos personales en la construcción europea es que la primera vez que el Tribunal de Justicia de la Unión Europea afirma que los derechos fundamentales son principios generales del Derecho comunitario fue el caso *Stauder* una sentencia de 1969 que resolvía un litigio de protección de datos personales. Posteriormente han sido muchos los instrumentos tanto de Derecho originario como derivado que han reconocido y desarrollado el derecho fundamental a la protección de datos personales en la Unión Europea, a lo que se ha unido una interesante jurisprudencia del Tribunal de Justicia que ha analizado de manera indirecta este derecho fundamental[210].

El diálogo en diferentes ámbitos –sea académico o judicial– contribuyó en el marco europeo, no solamente a configurar el contenido del derecho a la protección de datos sino que, además, obligó a establecer estándares comunes que aseguren en

[205] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 88.
[206] Troncoso, "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional".
[207] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 20.
[208] Arenas Ramiro, "La protección de datos personales en los países de la Unión Europea", 136.
[209] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 17.
[210] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 38-39.

cada Estado la plena satisfacción de los bienes jurídicos, que se desprenden de este instituto de garantía. En todo caso, sin olvidar las exigencias que plantea este derecho fundamental en la sociedad digital, consideramos que en la Unión Europea su evolución se produjo "como consecuencia del desarrollo tecnológico y su impacto en los derechos fundamentales, cuando se advierten las ventajas y desventajas que el uso de las nuevas tecnologías, en especial la informática, representan para la vida privada de las personas"[211].

Siguiendo a Mónica Arenas, advertimos un reconocimiento diverso en los Estados de la Unión Europea. Aquellos en el que el derecho a la protección de datos forma parte del contenido de otros derechos –por ejemplo, la intimidad– y otros en los que la protección de datos se constituye como un derecho autónomo. Arenas clasifica a los Estados de la Unión Europea en tres grupos. Un primer grupo, formado por los Estados en los que la Constitución reconoce, expresamente, el derecho a la protección de datos: Suecia, Portugal, Eslovaquia, Eslovenia, Hungría y Polonia. El segundo grupo, en el que la Constitución no reconoce este derecho, pero sí establece disposiciones sobre la materia –por ejemplo, un mandato al legislador–, el cual ha permitido al Tribunal Constitucional reconocer a la protección de datos como un derecho fundamental: España, Países Bajos, Finlandia y Lituania. Y, un tercer grupo, en donde la Constitución no hace ninguna referencia a la protección de datos. Aquí, el Tribunal Constitucional ha reconocido a la protección de datos como parte integrante de otro derecho fundamental –por ejemplo, ya sea el derecho a la intimidad o a la vida privada, al libre desarrollo de la personalidad y a la dignidad humana– sí contemplado en la Constitución. En este último grupo se encontraría la mayoría de los Estados miembros de la Unión Europea, por ejemplo, Italia[212].

[211] Arenas Ramiro, "La protección de datos personales en los países de la Unión Europea", 128.

[212] Cfr. Mónica Arenas Ramiro, "La protección de datos personales en los países de la Unión Europea". 129-130 En este punto, Antonio Troncoso advierte que Portugal (1976) fue el primer Estado europeo en contemplar de manera específica la protección de datos personales; le sigue, el Reino de los países bajos (1983), Finlandia (1980), Suecia (1994); mientras que Italia y Alemania –considerando incluso la falta de reconocimiento del derecho a la intimidad desde el ámbito constitucional- configuraron la protección de este derecho en virtud de la jurisprudencia desarrollada por los Tribunales Constitucionales. Cfr. Antonio Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 49-50**.**

Por otra parte, “la construcción europea, que requiere ineludiblemente la constitución del mercado interior, exige que se garantice la libre circulación de los datos personales, dado el valor económico que los mismos tienen en las transacciones comerciales”[213]. Considerando este aspecto, destacamos que “la máxima expresión del reconocimiento de este derecho por la puerta trasera se alcanza con la mismísima Directiva 95/46/CE (…) La directiva sustentaba su base legal en la libertad de circulación y en la proscripción de obstáculos que impidieran tal fin”[214]. En efecto, otra de las características por las que el derecho a la protección de datos, tiende a consolidarse como un derecho global que responde a las circunstancias internacionales, es el aseguramiento de su tutela en procesos que resultan de la integración comercial supranacional. Por ello, “fundamentalmente se entendió que las diferencias entre las Leyes de Protección de Datos de los Estados miembros serían un obstáculo para el flujo interno de datos personales”[215].

Precisamente, a este fin respondió “la Directiva 95/46/CEE de la que deriva la legislación de los países europeos en materia de protección de datos, y en particular, en España, la Ley Orgánica 15/1999 de 13 de diciembre”[216]. Por consiguiente, señalamos que:

> La Directiva 95/46/CE iba encaminada a alcanzar dos de las ambiciones más antiguas del proyecto de integración europea: la realización del mercado interior -en este caso, la libre circulación de datos personales- y la protección de los derechos y libertades fundamentales de las personas físicas en lo que respecta al tratamiento de datos personales[217].

---

[213] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 90-91.
[214] Rallo Lombarte, “El nuevo derecho a la protección de datos”, 51.
[215] Gregorio, “Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina”, 309.
[216] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 92.
[217] Troncoso, “Hacia un nuevo marco jurídico europeo de la protección de datos personales”, 37. A esto, agregamos que “para la directiva, la eliminación de los obstáculos a la circulación de datos personales como objetivo esencial para el mercado interior obligaba a coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales fuera regulado de forma coherente y no obstaculizara la libre circulación de datos personales excusando la protección de los derechos y libertades de las personas físicas. En definitiva, la protección de datos constituía, en apariencia, un objetivo secundario frente a un fin principal: garantizar la libre circulación para preservar el correcto funcionamiento del mercado interior de la Unión Europea. Cfr. Rallo Lombarte, “El nuevo derecho a la protección de datos”, 51-52.

Ahora bien, por una parte, especial relevancia tiene la Carta de los Derechos Fundamentales de la Unión Europea que reconoce a la protección de datos personales, como un derecho fundamental autónomo y, por la cual dispone "ninguna referencia a la intimidad o privacidad; ninguna a la informática. Sí una previsión expresa, de suma importancia, al hecho de que <El respeto de estas normas [sobre protección de datos] quedará sujeto al control de una autoridad independiente>"[218].

Y, por otra, precisamos que el desarrollo de este derecho fundamental ha desembocado en la aprobación del RGPD, por el que se deroga la Directiva 95/46/CE, y que fue aprobado el 27 de abril de 2016 en Bruselas.

> Se ha dicho que el nuevo Reglamento supone un giro copernicano respecto a la situación anterior. Cierto que la gran mayoría de los principios y fundamentos de la Directiva, por no decir todos, siguen estando en la base misma de la protección de datos en Europa y que el contenido esencial del derecho a la protección de datos, reconocido en el artículo 8 de la Carta Europea de Derechos Humanos, sigue siendo principalmente el mismo. Pero el Reglamento introduce, a veces directamente, a veces de forma algo soterrada, un nuevo modelo de protección de datos para Europa[219].

Es evidente el desarrollo normativo –no solo desde el ámbito interno de cada Estado, sino desde el marco común europeo– tendente a desarrollar el derecho fundamental a la protección de datos, por lo que a continuación se abordarán los aspectos jurídicos más significativos de la Carta de Derechos y del RGPD.

### 3.1 La Carta de Derechos de la Unión Europea y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE

Como queda expuesto, a consecuencia de los avances tecnológicos y procesos de integración comercial que han derivado en el tratamiento de la información personal dentro de una sociedad automatizada, la protección de datos ha llegado a

[218] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 93-94.
[219] José Luis Piñar Mañas, "Introducción. Hacia un nuevo modelo europeo de protección de datos", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 14.

constituirse como uno de los derechos globales y/o supranacionales que requieren especial observancia, dentro de la comunidad internacional.

> La derogación de la Directiva 95/46/CE y de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su sustitución por el RGPD y la LOPDGDD invitan a una sugestiva reflexión sobre el impacto nacional de esta ambiciosa reforma legislativa tanto en el plano del sistema de fuentes normadoras del derecho de protección de datos y de su alcance constitucional como sobre los novedosos rasgos conformadores de la garantía efectiva de este derecho[220].

Esto conlleva a la necesidad de contemplar, desde el Estado un marco de protección y garantía de los derechos vinculados con la protección de datos personales; por cuanto los ordenamientos jurídicos deben propender hacia un régimen legislativo que garantice este derecho, tanto desde el ámbito constitucional como en el régimen sectorial, con la finalidad de hacer efectiva a la protección de la información, a través de sistemas de calidad y eficiencia en beneficio de los derechos que corresponden a los ciudadanos.

Tomando en cuenta la dimensión internacional del derecho a la protección de datos, se precisa un equilibrio no sólo de la normativa nacional, sino también supranacional. Por ello, en la era de la economía digital y de las tecnologías de la información y comunicación, insistimos en la protección integral de la persona, por cuanto la tutela de la información personal es fundamental "para garantizar la protección de otros derechos humanos y libertades fundamentales, toda vez que redunda, a fin de cuentas, en la dignidad de la persona"[221].

Por ello, en este punto, apreciamos que:

> La normativa europea y nacional de protección de datos regula y define los ficheros de datos personales –aunque también albergue el concepto de tratamiento-, algo característico de la primera etapa de desarrollo de la informática dominada por los grandes ordenadores –la de la macro informática- y de la segunda etapa caracterizada por la extensión de los ordenadores personales –la de la micro-informática-, pero no alcanza a regular y ni siquiera a entrever las siguientes grandes etapas en la historia de la informática caracterizadas por el desarrollo y la rapidez de Internet, por los eficaces motores de búsqueda, por la aparición y universalización de las redes sociales virtuales, por los servicios de computación en nube –*Cloud Computing*- o por la reciente problemática que supone el denominado "Internet de las Cosas" –*Internet of Things*–"[222].

[220] Rallo Lombarte, "El nuevo derecho a la protección de datos", 48.
[221] Maqueo Ramírez, Moreno y Recio Gayo, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", 93.
[222] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 35.

Es esencial reforzar el contenido de este derecho fundamental sobre aquello que pueda advertir una amenaza. “No lo parece. Pero hay que reconocer que los elementos que hacen reconocible este derecho y el sistema de garantías que lo ampara han sufrido transformaciones extraordinarias”[223]. Esto es trascendental, cuando se sabe que el avance digital resulta vertiginoso en relación a la normativa que se pueda desarrollar sobre esta materia. En este sentido, en el marco de la Unión Europea este derecho ha generado gran diversidad normativa, que es necesario mencionar con el fin de contextualizar, más adelante, el estado de la situación en España.

En primer término, estimamos que:

> La idea de dotar a la Unión Europea de un catálogo propio de derechos fundamentales toma cuerpo en las sesiones del Consejo Europeo de Colonia y Tampere en 1999. Aprovechando esta coyuntura, el Grupo de Trabajo del art. 29, que como se ha visto *supra* fue creado por la Directiva 95/46, a través de su Dictamen 4/99, de 7 de septiembre, recomienda la inclusión del derecho fundamental a la protección de datos en el futuro catálogo europeo de derechos fundamentales[224].

Así, la Carta de Derechos Fundamentales de la Unión Europea (2000/C 364/01) en el art. 8 reconoce, propiamente, el derecho a la protección de datos de carácter personal, considerando que:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Esta definición supone, “desde el punto de vista jurídico, una expresión común para designar el derecho de las personas a proteger sus informaciones personales y, desde el punto de vista político, implica la aceptación de un vocablo común para todos los estados miembros”[225]. Además, la importancia de este reconocimiento radica en que, a más considerar a la protección de datos como derecho autónomo,

---

[223] Rallo Lombarte, “El nuevo derecho a la protección de datos”, 48-49.

[224] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 263.

[225] María Mercedes Serrano Pérez, “El derecho fundamental a la protección de datos. Su contenido esencial”, *Anuario multidisciplinar para la modernización de las Administraciones Públicas*, Nro. 1 (2005): 252.

se promueve el respeto de un conjunto de principios para su tutela. Se hace referencia a los principios de lealtad, finalidad y consentimiento. Además, se reconoce, expresamente, la facultad de ejercer el derecho a la rectificación de la información personal materializada, por medio de la garantía del *habeas data*. De esta manera, esta declaración "amparó la abducción de este derecho por instancias europeas para convertirlo en un derecho europeo, homogéneo y común, sustancialmente desposeído de base estatal constitucional y legislativa —salvo en los estrechos márgenes residuales que su conformación jurídica europea permitiera—"[226]. En todo caso, también se le atribuye a la Carta de Derechos Fundamentales de la Unión Europea haber desplazado "finalmente a los partidarios de reconocer la necesidad de proteger los datos de las personas entendiéndolo como una extensión de la intimidad"[227].

Por otra parte, la Carta determina que el respeto del derecho a la protección de datos estará sujeto al control de una autoridad independiente. En este punto, entendemos que "esta garantía institucional es considerada por los órganos legislativos de la UE, en toda su actividad normativa dirigida a la protección de datos, como la instancia más adecuada para la tutela de este derecho fundamental de los ciudadanos europeos"[228].

Ahora bien, en 2007, el texto de la Carta de Derechos Fundamentales de la Unión Europea fue ratificado en Estrasburgo, y consecuentemente, en 2009 pasa a formar parte del contenido del Tratado de Lisboa. Así, el Tratado de Funcionamiento de la Unión Europea, que fue introducido por el Tratado de Lisboa, reconoce que:

> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
> 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes –art. 16–.

[226] Rallo Lombarte, "El nuevo derecho a la protección de datos", 53-54.
[227] Serrano Pérez, "El derecho fundamental a la protección de datos. Su contenido esencial", 252.
[228] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 266.

Al respecto, afirmamos que:

> El carácter vinculante que el Tratado de Lisboa ha dado a la Carta de Derechos Fundamentales de la Unión Europea, que en el art. 8 consagra el derecho a la protección de los datos de carácter personal de manera autónoma al derecho al respeto a la vida privada y familiar reconocido en el art. 7, refuerza las bases jurídicas específicas para que la Unión Europea apruebe una normativa sobre protección de datos personales aplicable a todos los ámbitos, suprimiendo las limitaciones establecidas en la Directiva[229].

Finalmente, el RGPD precisa la inserción de nuevas bases relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos[230]. "Constituye un desarrollo completo y exhaustivo del derecho de protección de datos reconocido en el art. 8 CDFUE. La elección de este instrumento jurídico para garantizar el derecho comporta una voluntad excluyente de cualquier intervención estatal dirigida a regular este derecho fundamental"[231]. Por tanto, a la luz de este instrumento se define "un nuevo modelo europeo de protección de datos. Protección respecto de la que por supuesto ninguna duda cabe albergar acerca de su naturaleza de verdadero derecho fundamental[232]. La evolución tecnológica, el entorno globalizador, la economía digital constituyen sus principales motivaciones[233] y que, según el RGPD:

---

[229] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 34-35. Hay que considerar que "la existencia de esta incuestionada nueva base jurídica no implicaba necesariamente alterar el statu quo y optar por instrumentos jurídicos diferentes a la directiva para reformar el sistema europeo de protección de datos. Sin embargo, para sorpresa generalizada y sin oposición significativa, la Comisión Europea postuló el reglamento como instrumento idóneo y adoptó la estrategia más ambiciosa para procurar la mayor homogeneización posible del sistema europeo de protección de datos". Cfr. Rallo Lombarte, "El nuevo derecho a la protección de datos", 55.

[230] El RGPD supuso la derogación de la Directiva 95/46 y, en el caso de España, la aprobación de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los Derechos Digitales, por la cual se deroga la Ley Orgánica 15/1999 de Protección de Datos Personales. Cabe señalar que, a la Ley Orgánica 3/2018 le antecedió el Real Decreto-Ley 5/2018 de medidas urgentes, para la adaptación del Derecho español a la normativa de la Unión Europea (Reglamento 2016/679) en materia de protección de datos.

[231] Rallo Lombarte, "El nuevo derecho a la protección de datos", 56.

[232] Piñar Mañas, "Introducción. Hacia un nuevo modelo europeo de protección de datos", 15.

[233] Con referencia a este aspecto, subrayamos que "el impacto de nuevas tecnologías como internet y los intereses empresariales transnacionales pesaron significativamente, pues habían resultado insistentes las críticas a la Directiva 95/46/CE que denunciaban la fragmentación nacional de la normativa de protección de datos que comportaba inseguridad jurídica, especialmente, en relación con las transferencias internacionales inherentes a una economía globalizada. El reglamento era, aparentemente, el instrumento jurídico idóneo por su alcance general, obligatoriedad en todos sus elementos y aplicabilidad directa en cada Estado miembro (art. 288 del TFUE) para impedir la fragmentación y garantizar la máxima seguridad jurídica". Cfr. Rallo Lombarte, "El nuevo derecho a la protección de datos", 55-56.

> Requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas –Considerando 7–.

Desde sus inicios, la formulación de este Reglamento tuvo criterios relevantes, a partir de las nuevas incorporaciones que se incluían, en virtud de los avances tecnológicos. Así, se advertía que:

> La propuesta de Reglamento tiene que ser bienvenida desde la perspectiva de las personas porque le da más instrumentos para el control sobre su información personal. El incremento de los tratamientos de datos personales derivado del proceso tecnológico .Internet de las cosas, video vigilancia, biometría, nanotecnología, historia clínica electrónica en la nube, RFID eleva el nivel de riesgo para la privacidad, por lo que este proceso debe ir acompañado de un fortalecimiento de las garantías de las personas en la era de Internet[234].

Con referencia a este aspecto, estimamos que el RGPD expresa "un reconocimiento implícito del modelo español de protección de datos personales y de la actividad de supervisión y control que ha desempeñado la Agencia Española de Protección de Datos en las últimas dos décadas"[235]. En este orden, no es extraño advertir que el marco jurídico para la protección de datos personales en España es un significativo resultado, tanto de la promulgación normativa que ha realizado la Unión Europea, como de los propios criterios jurisprudenciales del Tribunal Constitucional Español.

### 3.2 El caso de España

Bajo la categoría de "derechos fundamentales y libertades públicas", desde el ámbito constitucional se reconoce que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" –art. 18.4–. Esta declaración, "ha merecido un indudable reconocimiento por tratarse de un loable intento de actualización y adecuación de la normativa constitucional a las nuevas realidades sociales que afectaban al ser

[234] Piñar Mañas, "Introducción. Hacia un nuevo modelo europeo de protección de datos", 175.
[235] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 175.

humano en su dignidad y en el disfrute de sus derechos"[236]. Naturalmente, a la luz del art. 18.4, el derecho a la protección de datos personales "no resulta en sentido estricto de la creación de un nuevo derecho sino de la deducción, a partir de la limitación del uso de la informática de la existencia de un conjunto de facultades y posibilidades, esto es, de un contenido esencial que solo pueden encuadrarse bajo esta nueva categoría y que rebasa los límites de la intimidad"[237].

Por otra parte, la Constitución establece que los derechos fundamentales y las libertades públicas deben ser regulados, por medio de una Ley Orgánica[238]. En este ámbito, gran importancia tuvo la regulación establecida, tanto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal –LORTAD– como en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal –LOPD–[239]. No obstante, en la actualidad, la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los Derechos Digitales desarrolla y regula, no solamente el derecho a la protección de datos sino también la garantía de los derechos digitales vinculados al tratamiento de la información personal[240]. Al respecto, anotamos que "ha sido la

[236] Artemi Rallo Lombarte, "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)", *UNED: Revista de Derecho Político*, Nro. 100 (2017), 639-669.
[237] Serrano Pérez, "El derecho fundamental a la protección de datos. Su contenido esencial", 251.
[238] Al respecto, la Constitución Española señala que: "Son Leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas, las que aprueben los Estatutos de Autonomía y el régimen electoral general y las demás previstas en la Constitución" –art. 81–.
[239] Estas normas estuvieron "inspiradas en las legislaciones de los países europeos y, especialmente, en la normativa internacional: La LORTAD se inspiró en el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal; la LOPD es transposición de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos". Cfr. Antonio Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 82. En todo caso, "son reconocidas con el honroso título de normas de desarrollo del precepto constitucional que consagra la garantía de los derechos frente al uso de la informática. Tal reconocimiento resulta notablemente deudor de la hermenéutica constitucional que, del mandato constitucional dirigido a los poderes públicos para preservar a los individuos frente a los riesgos y amenazas de la tecnología, dedujo con valentía y determinación un derecho fundamental autónomo —denominado, inicialmente y con singular originalidad, libertad informática y, posteriormente, en forma más prosaica, derecho a la protección de datos— de efectos expansivos extraordinarios". Cfr. Rallo Lombarte, "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)", 642-643.
[240] Corresponde precisar que la aprobación del RGPD "exigía adecuar el derecho español a esta norma de derecho derivado institucional de la Unión Europea que es obligatoria en todos sus elementos y directamente aplicable. El RGPD desplaza la normativa nacional que sea incompatible

LOPDGDD la que ha llevado a cabo un desarrollo del derecho a la protección de datos personales en el marco del ordenamiento constitucional, teniendo en cuenta otros derechos y bienes constitucionales"[241]. Por tanto, "ha venido a alumbrar un nuevo marco normativo, europeo y nacional, de garantía del derecho a la protección de datos"[242].

En relación a la autoridad de control, destacamos a la Agencia Española de Protección de Datos (AEPD). Desde el ámbito orgánico, en el marco de la estructura estatal y sin perjuicio de las creadas en las administraciones de las Comunidades Autónomas, esta autoridad se encarga de cumplir con los objetivos de la normativa para la protección de datos[243]. Su importancia es asumida dentro de los cambios del RGPD por lo que se espera mayor fortalecimiento de los mecanismos de control, frente a la garantía de este derecho fundamental. Así, por ejemplo, destacamos que "el establecimiento por el RGPD de mecanismos de cooperación y coherencia entre autoridades de control facilitará, sin duda, una interpretación homogénea de esta norma europea por las autoridades nacionales de protección de datos, aportando soluciones que ayuden a la convergencia"[244].

En cuanto a la normativa que desarrolla y regula el derecho a la protección de datos, la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los

---

con éste por el principio de primacía y el efecto directo del Derecho europeo. Esto significa que los responsables de tratamientos, las autoridades de protección de datos y los tribunales estarán obligados a inaplicar los preceptos de la LOPD y del RLOPD que sean incompatibles con el RGPD y aplicar lo previsto en el RGPD. Sin embargo, el RGPD no deroga las normas nacionales incompatibles porque la primacía del derecho europeo no es supremacía y no afecta a la validez de las normas internas. Por ello, por razones de seguridad jurídica, corresponde al legislador y al Gobierno derogar las normas de derecho interno incompatibles con el Derecho de la Unión Europea.2 De esta forma, no debían mantenerse normas nacionales contrarias al RGPD, aunque los poderes públicos procedan a su inaplicación". Cfr. Antonio Troncoso, "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de Derechos Digitales", *Derecom*, Nro. 26 (2019): 131-140.

[241] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 251.

[242] Rallo Lombarte, "El nuevo derecho a la protección de datos", 48.

[243] Su estatuto se aprueba, bajo Real Decreto 428/1993 y modificado por los Reales Decretos de 1665/2008 y 156/1996.

[244] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 197.

Derechos Digitales plantea en su objeto: “adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679”, completando sus disposiciones; garantizar “el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución” con arreglo “a lo establecido en el Reglamento (UE) 2016/679”; y finalmente, garantizar “los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución” –art. 1–.

En este sentido, subrayamos que:

> La LOPDGDD, a diferencia del RGPD, extiende su objeto más allá del derecho fundamental a la protección de datos personales porque trata de “garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el art. 18.4 CE” –art. 1.b–. Por ese motivo, su ámbito de aplicación no se circunscribe a los tratamientos de datos personales en el caso del Título X “Garantía de los derechos digitales”, salvo los artículos 89 al 94 para los que sí se exige el tratamiento de datos personales. Esto es una manifestación de que no se trata de una Ley Orgánica sólo de Protección de Datos Personales sino también de garantía de los derechos digitales[245].

Así también la Ley Orgánica 3/2018 dispone que en relación al tratamiento de la información personal “se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero” –art. 2.1–. De esta manera, esta Ley advierte “el derecho fundamental a la protección de datos personales no tiene como objeto, valga la redundancia, proteger los datos personales sino sólo cuando éstos sean sometidos a tratamiento”[246].

Por otra parte, la Constitución señala que “los derechos y libertades reconocidos en el Capítulo segundo del presente Título vinculan a todos los poderes públicos” –art. 53–. Consecuentemente, el régimen de la Administración Pública debe atender, en primera instancia, al mandato constitucional y luego a la regulación que la Ley Orgánica 3/2018 dispone dentro del régimen de protección de datos. En este sentido, reiteramos que este derecho fundamental se orienta a:

> Garantizar al individuo el derecho a organizar y determinar por sí mismo aspectos esenciales de su vida, como a quién y en qué momento quiere comunicar cuestiones personales,

[245] Ibíd., 198-199.
[246] Ibíd., 199.

> pensamientos, sentimientos o emociones, o incluso su identidad. El fundamento último de este derecho es la dignidad de la persona —en lo que coincide con el derecho a la intimidad y con la mayoría de los derechos fundamentales— y el libre desarrollo de la personalidad, sin los que se priva a la persona del disfrute de los demás derechos fundamentales[247].

Finalmente, en el marco jurídico español, forzosamente, debemos citar algunas referencias que la jurisprudencia española ha resuelto en materia de protección de datos personales[248]. "Aunque, inicialmente, el Tribunal Constitucional calificaba este derecho como una especificación del derecho a la intimidad, pronto le otorgó la naturaleza de un derecho fundamental autónomo"[249]. Uno de los más importantes criterios que instituyó el enmarque constitucional del derecho a la protección de datos personales fue la STC 292/2000[250]. Con referencia a este punto, recordemos que:

> A partir de aquí, la STC 292/2000, despeja ya las ambigüedades y establece rotundamente que lo que ya había considerado anteriormente "un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos" constituye, también, "un derecho o libertad fundamental". Es, prosigue la sentencia, "lo que se ha dado en llamar –libertad informática-, la cual, precisa, posee "una dimensión positiva

[247] Arenas Ramiro, "La protección de datos personales en los países de la Unión Europea", 130.

[248] Es importante señalar que, "el art. 18.4 CE se limita a mandatar al legislador para que garantice los derechos fundamentales frente al uso de la informática y, a diferencia de la Constitución portuguesa, ni explicita el reconocimiento del derecho de protección de datos ni asegura un contenido constitucional mínimo del mismo. Pero el Tribunal Constitucional se ha encargado de anclar en este precepto constitucional el reconocimiento de un derecho fundamental autónomo a la protección de datos personales". Cfr. Rallo Lombarte, "El nuevo derecho a la protección de datos", 56-57.

[249] Rallo Lombarte, "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)", 649.

[250] En todo caso, advertimos que el primer precedente del Tribunal Constitucional se fundó en su Sentencia 254/93, en donde proclamó que: "nuestra CE ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la CE llama «la informática»". Véase la Sentencia 254/1993, de 20 de julio de 1993. Recurso de amparo 1827/1990. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-T-1993-21425. "No obstante, ni en esa Sentencia, ni, sobre todo, en la 143/1994 –que se ocupa del Número de Identificación Fiscal– se acierta a distinguir nítidamente la protección de datos de carácter personal del derecho a la intimidad. Será preciso esperar al grupo de Sentencias que se abre con la 11/1998, para que el Tribunal Constitucional profundice en el sentido que tiene el derecho reconocido por la LORTAD y vaya preparando su afirmación como derecho fundamental en la Sentencia 292/2000". Cfr. Pablo Lucas Murillo de la Cueva, "El derecho a la autodeterminación informativa y la protección de datos personales", *Eusko Ikaskuntza. Miramar Jauregia. Miraconcha*, Nro. 20 (2008), 43-58.

> que excede el ámbito propio del derecho fundamental a la intimidad (…) y (…) se traduce en un derecho de control sobre los datos relativos a la propia persona"[251].

Bajo estas apreciaciones, la conceptualización de este derecho en el ordenamiento jurídico español tiene como principal característica "la confluencia de factores de distinta naturaleza (legislativa, judicial, política) y ámbito (estatal, comunitario, internacional) la que explica la decisión de nuestro Tribunal Constitucional de reconocer un nuevo derecho fundamental a la protección de datos personales como categoría autónoma"[252], garantizando, de esta manera, "un ámbito más idóneo —que el que podían ofrecer, por sí mismos, los derechos fundamentales al honor, a la intimidad y a la propia imagen reconocidos en el artículo 18 CE— ante la eclosión de nuevos peligros que las nuevas tecnologías pueden suponer"[253].

Por ahora, el análisis de la legislación en España queda fijado hasta este punto, por cuanto en los siguientes capítulos particular interés representa contrastar ésta con la legislación ecuatoriana. A la luz de los principales instrumentos internacionales y la normativa de protección de datos en Ecuador, en adelante, pretendemos estimar las bases de un modelo de regulación que contenga los principios fundamentales, conforme a los niveles adecuados que la comunidad internacional reconoce como necesarios para garantizar de manera integral el derecho a la protección de datos.

[251] Lucas Murillo de la Cueva y Piñar Mañas, *El derecho a la autodeterminación informativa,* 33-34.
[252] Ibíd., 43.
[253] Rallo Lombarte, "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)", 652.

## CAPÍTULO III: ESTUDIO DE LA NORMATIVA QUE DESARROLLA EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES EN ECUADOR, DESDE UNA PERSPECTIVA SECTORIAL

### 1. Introducción

En el marco de protección de la información de carácter personal, el desarrollo de este derecho fundamental tiene su origen, tanto en Leyes generales, como en aquellas que forman parte del ámbito de la normativa sectorial. En ambos casos, el objeto de esta regulación es establecer garantías, confianza y seguridad jurídica que permitan a los ciudadanos ejercer el control y el dominio de la información personal, frente a su tratamiento en el ámbito público y privado.

La Organización de los Estados Americanos –en adelante OEA– señala que cada Estado miembro determinará la mejor manera de implementar en los ordenamientos jurídicos internos los principios que se recomiendan en la Guía Legislativa de 2015, sea, a través de Leyes, normas u otros mecanismos[1]. Así también los Estándares de protección de datos personales para los Estados Iberoamericanos de 2017 reconocen la necesidad de armonizar los ordenamientos jurídicos en cuanto a la definición, principios, derechos y procedimientos que componen el derecho a la protección de datos[2]. Adicionalmente, el Reglamento (UE) 2016/679 –en adelante RGPD– reconoce que, además de armonizar la legislación de protección de datos personales, mediante una normativa general, existe un margen de maniobra para una regulación más específica por medio de una normativa sectorial[3].

[1] La Guía Legislativa de la OEA recomienda que "los Estados Miembros deben establecer reglas efectivas para la protección de datos personales que den efecto al derecho de la persona a la privacidad y que respeten sus datos personales, protegiendo al mismo tiempo el derecho de la persona a beneficiarse del libre flujo de información y del acceso a la economía digital". Véase, Guía Legislativa para los Estados Miembros de la OEA (Principios de Privacidad y Protección de Datos Personales en las Américas): Recuperado de: http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

[2] Los Estándares de protección de datos personales para los Estados Iberoamericanos de 2017 precisan que la falta de armonización de las legislaciones nacionales "dificulta actualmente hacer frente a los nuevos retos y desafíos para la protección de este derecho derivados de la constante y vertiginosa evolución tecnológica y la globalización en diversos ámbitos" –Considerando 9–.

[3] El RGPD establece "un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos

Los ordenamientos jurídicos, sobre protección de datos personales evidencian la consolidación de un modelo mixto sustentado en la existencia de una Ley general y una pluralidad de normas específicas, también denominada normativa sectorial. A partir de este modelo, la Ley general de protección de datos se orienta a garantizar y desarrollar este derecho fundamental, mientras que la normativa sectorial se adapta mejor a las situaciones específicas que requieren la regulación del tratamiento de la información personal[4].

Como apreciamos:

> El modelo mixto de norma general y remisión a normas sectoriales precedentes permite, además, abreviar las normas generales, que así no tienen la necesidad de reproducir ni derogar la normativa sectorial precedente y que pueden diferir en la regulación sectorial futura aspectos nuevos sobre informática y protección de datos[5].

En el caso de Ecuador, previo a la aprobación de la Ley Orgánica de Protección de Datos Personales de 2021, antes y después del reconocimiento constitucional del derecho a la protección de datos personales en 2008, el orden jurídico para la tutela de este derecho estuvo desarrollado, únicamente, en la normativa sectorial y en algunos precedentes de la Corte Constitucional. No obstante, tres han sido los proyectos que han impulsado la materialización de una Ley general.

El Proyecto de Ley presentado en 2010, sobre protección a la Intimidad y a los Datos personales, se promovió sobre la base de la reforma constitucional de 2008, en lo que respecta al derecho a la protección de datos y la garantía jurisdiccional del *habeas data*. Fundamentalmente, la evolución de las tecnologías de la información y la comunicación, frente al tratamiento automatizado de la información personal fueron las principales motivaciones de este proyecto. No obstante, luego del procedimiento parlamentario, en 2012 la Comisión Especializada Permanente de

sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito" –Considerando 10–.

[4] Cfr. Antonio Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, (Valencia: Tirant lo Blanch, 2010),87.

[5] Ibíd.

Justicia y Estructura del Estado resolvió en segundo debate recomendar al Pleno de la Asamblea Nacional archivar el proyecto.

Los principales argumentos para el archivo de este primer proyecto se fundaron en considerar que: primero, el proyecto no tenía la condición de Ley orgánica, a pesar de contener una normativa que desarrollaba derechos fundamentales relacionados con la protección de datos; segundo, la creación de un órgano de control o de una autoridad nacional de protección incrementaría más burocracia; y tercero, la nueva normativa supondría una innecesaria expansión y repetición de acciones judiciales constitucionales y ordinarias, que ya se encontraban reconocidas en el ordenamiento jurídico nacional[6].

En cuanto al proyecto de 2016, este fue calificado por el Consejo de Administración Legislativa y remitido a la Comisión Especializada Permanente de Justicia y Estructura del Estado, para el inicio del trámite legislativo. En su exposición de motivos, tanto el desarrollo de las tecnologías de la información y comunicación como el flujo transnacional de que pueden ser objeto los datos personales, fueron las bases por las cuales se formuló dicha propuesta. Esta segunda propuesta no mereció ningún informe de la Comisión. Como prescribe la Ley Orgánica de la Función Legislativa, tampoco se consideró la necesidad de que los ciudadanos acudan ante la Comisión, en virtud del interés social que representa una Ley de este estilo[7].

Finalmente, el proyecto de “Ley Orgánica de Protección de Datos Personales” presentado en 2019 por el ejecutivo, el cual ha desembocado en la actual Ley

[6] Puede consultarse el texto completo del Proyecto de Ley de 2010, a través de la página oficial de la Asamblea Nacional: https://Leyes.asambleanacional.gob.ec/

[7] La Ley Orgánica de la Función Legislativa (art. 58) prescribe que: “Las comisiones especializadas dentro del plazo máximo de cuarenta y cinco días contados a partir de la fecha de inicio del tratamiento del proyecto de Ley, presentarán a la Presidenta o Presidente de la Asamblea Nacional sus informes con las observaciones que juzguen necesarias introducir. Dentro del referido plazo, se deberá considerar un tiempo no menor a los quince primeros días, para que las ciudadanas y los ciudadanos que tengan interés en la aprobación del proyecto de Ley, o que consideren que sus derechos puedan ser afectados por su expedición, puedan acudir ante la comisión especializada y exponer sus argumentos” –art. 58–. Sobre el estado actual y trámite del proyecto de 2016 puede consultarse el sitio Web de la Asamblea Nacional: https://Leyes.asambleanacional.gob.ec/.

general de protección de datos, responde a la necesidad de contar con una legislación especializada que concrete el derecho a la protección de datos y promueva –en el ámbito público y privado– la cooperación económica y comercial internacional, garantizando el flujo transfronterizo de datos personales[8]. En todo caso, precisamos que este tercer proyecto fue presentado, a partir del escándalo que vincula a varias instituciones públicas y privadas como responsables de la filtración de datos, de casi la totalidad de la población ecuatoriana, incluidos, aproximadamente, 6.7 millones de registros que corresponden a menores de edad[9].

Ahora bien, desde el régimen sectorial se destacan –antes de la Reforma Constitucional de 2008–, la Ley Orgánica de la Salud; Ley de Seguridad Social; Ley de Comercio Electrónico, Firmas y Mensajes de Datos; Código de la Niñez y la Adolescencia, entre otras. Posterior a dicha reforma, el Código Orgánico Integral Penal; Código Orgánico General de Procesos; Ley Orgánica Electoral o Código de la Democracia; Ley del Sistema Nacional de Registro de Datos Públicos; Ley Orgánica de Comunicación y Ley Orgánica de Telecomunicaciones.

Como hemos destacado en otro momento, la protección de datos personales requiere de un marco jurídico integral que garantice una tutela coherente y homogénea. Naturalmente, en torno al desarrollo tecnológico y fortalecimiento de los procesos de integración económica y comercial, se busca que las legislaciones nacionales respondan con garantías que protejan los derechos y libertades que se desprenden de este instituto de garantía. Si bien la normativa sectorial facilita la regulación de determinados tratamientos específicos, señalamos que la existencia de una Ley general es necesaria, en virtud de que “tiene la ventaja de facilitar la configuración de un ordenamiento jurídico de protección de datos, que permita una

[8] El texto del Proyecto de Ley de 2019 también puede consultarse en la página de la Asamblea Nacional: https://Leyes.asambleanacional.gob.ec/. Esta propuesta, al igual que la presentada en 2016, fue calificada por el Consejo de Administración Legislativa y remitida a la Comisión Especializada de Soberanía, Integración, Relaciones Internacionales y Seguridad Integral, para el inicio del trámite y tratamiento legislativo; y como hemos indicado, ha sido aprobada, finalmente.

[9] La filtración de datos personales de casi la totalidad de la población ecuatoriana tuvo gran repercusión en el contexto internacional: Fue reportada por los principales medios de comunicación, tanto nacional como internacional. Véase: https://www.bbc.com/news/technology-49715478; https://tinyurl.com/yxvrllr6; https://tinyurl.com/rw7g7ar.

interpretación uniforme y reduzca el riesgo de incoherencias"[10]. Por tanto, subrayamos que, antes de la aprobación de la Ley general de 2021, verdaderamente, el legislador estaba "en deuda con los habitantes del Ecuador en materia de protección de datos personales, aunque las experiencias en la aplicación de las Leyes citadas pueden ser utilidad para una Ley general, sobre esta materia"[11].

De esta forma, frente al nuevo marco normativo de protección de datos, convendría preguntarse qué importancia seguirá teniendo el reconocimiento que realiza la Constitución de 2008, sobre el derecho a la protección de datos, el cual, además, se ha desarrollado en varias Leyes sectoriales y algunos precedentes de la Corte Constitucional; y qué presupuestos precisa esta Ley general, para el ámbito sectorial, atendiendo el paradigma del Estado constitucional de derechos y justicia.

No es el momento de analizar la pertinencia de los proyectos presentados en 2016 y 2019, por cuanto serán objeto de análisis en los subsiguientes capítulos. No obstante, si conviene citar los argumentos bajos los cuales se resolvió el archivo del proyecto de 2010.

En primer lugar, una Ley de protección de datos–al sistematizar el derecho reconocido por la Constitución de 2008– tiene el carácter o condición de una Ley orgánica. Según señala el art. 133.2 de la Constitución, son Leyes orgánicas las que regulen el ejercicio de los derechos y garantías constitucionales. Por ello, entendemos que la protección de la información personal comprende el ejercicio de un derecho fundamental y de una garantía constitucional, reconocidos, a través de los arts. 66.19 y 92 de la Constitución. En segundo lugar, la creación de un órgano de control o autoridad nacional de protección de datos, no constituye una justificación para limitar la aprobación de una Ley general. Al contrario, consideramos al "principio de control independiente" o de las autoridades de protección de datos como uno de los pilares del marco regulador de este derecho.

[10] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 86**.**
[11] Julio Cesar Trujillo, "Las Garantías Jurisdiccionales", Recuperado de: Base de datos: Vlex.com.ec: https://app.vlex.com/#WW/vid/515951146/graphical_version.

Además, en el contexto internacional, su existencia representa una característica del nivel adecuado de tutela y garantía que exige la protección de datos personales.

Finalmente, la existencia de normativa sectorial no limita la aplicación de una Ley general. Una Ley de protección de datos deviene de la necesidad de garantizar unidad, coherencia y seguridad jurídica del marco de protección de la información de carácter personal. Por tanto, destacamos que la importancia de la normativa sectorial radica en que ésta facilita la regulación de tratamientos específicos, pero que se provee de una Ley general para garantizar una regulación homogénea y uniforme. A partir de las características que se desprenden de un sistema mixto compuesto por una Ley general y Leyes sectoriales, distinguimos la relevancia de un ordenamiento jurídico flexible en la materia, el cual "permite a los órganos encargados de su interpretación y aplicación, en especial a las Agencias de Protección de Datos, adaptar los principios a las situaciones que sucesivamente se presenten"[12]. Así, las Recomendaciones, Dictámenes, Directivas, Instrucciones o Resoluciones, por ejemplo, de las autoridades de supervisión y control pueden, además, coadyuvar a la aplicación de la legislación de protección de datos.

Si bien la nueva normativa de protección de datos introducirá importante cambios en el régimen sectorial, además, hay que tomar en consideración que la Constitución dispone que "el contenido de los derechos se desarrollará de manera progresiva a través de las normas, la jurisprudencia y las políticas públicas" –art. 11.8–; y que, también "en materia de derechos y garantías constitucionales, las servidoras y servidores públicos, administrativos o judiciales, deberán aplicar la norma y la interpretación que más favorezcan su efectiva vigencia" –art. 11.5–. Por ello, es necesario realizar un estudio pormenorizado de la normativa sectorial que el ordenamiento jurídico ecuatoriano ha desarrollado sobre este derecho fundamental, bien como un derecho autónomo, o bien, mediante la protección de los bienes jurídicos relacionados con el tratamiento de datos de carácter personal.

Reconociendo, por una parte, que:

[12] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 94.

> Un aspecto esencial de cualquier Estado constitucional moderno es el de subordinación no solo formal o procedimental de los actos y normas de toda autoridad pública a la Constitución, sino su subordinación material, es decir, la conformidad de todos estos actos y normas a los derechos constitucionales, de los cuales deben ser su realización y nunca medios de su violación[13].

Y, recordando, por otra, que son principios para el ejercicio de los derechos, tanto el desarrollo progresivo en la normativa secundaria o sectorial como la aplicación e interpretación que más favorezca a su efectiva vigencia; es necesario analizar si el derecho a la protección de datos personales está, correctamente, articulado en el ordenamiento jurídico sectorial. De igual manera, concretaríamos si éste –en el ejercicio de la Administración Pública– responde a los principios generales que establece la comunidad internacional.

Así, el presente capítulo tiene por objeto matizar en el ámbito sectorial de Ecuador la evolución normativa sobre el derecho a la protección de datos. Especial referencia se hará a la Guía Legislativa de la OEA, al RGPD y a la legislación sectorial en España, con el objeto de precisar un modelo de regulación que responda a los principios que exige este derecho fundamental.

[13] Agustín Grijalva, *Constitucionalismo en Ecuador*, (Quito-Ecuador: Corte Constitucional para el Período de Transición, 2012), 81.

## 2. REGIMEN SECTORIAL QUE DESARROLLA EL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES EN ECUADOR

### 2.1 La protección de datos personales en el Sector de la Salud

#### A. Código de Ética Médica

Una de las primeras normas vinculadas con la protección de la información personal es el Código de Ética Médica[14]. Se promulgó con el fin de contar con un instrumento ético y jurídico que regule las obligaciones de los profesionales de la salud, en lo relativo a la protección integral de los pacientes[15]. Precisamente, uno de los escenarios de regulación es el tratamiento de la información personal de quienes son usuarios del sistema de salud pública. Así, corresponde señalar que "la gestión de la asistencia y de los servicios sanitarios en atención primaria, en atención especializada y en la urgencia exige necesariamente una acumulación masiva de información personal de los ciudadanos"[16].

El Código de Ética Médica considera que los documentos médicos relacionados con los pacientes, así como el registro de la información por otros medios, tanto en los consultores privados como en los servicios de salud, "deben ser manejados con carácter reservado. Al personal paramédico encargado de los mismos deberá instruirle que está obligado a guardar el secreto médico involucrado en dichos documentos" –art. 75–. Esta norma advierte la importancia del deber de confidencialidad en el ámbito sanitario "por las características de los datos a tratar

[14] El Código de Ética Médica fue aprobado, mediante el Acuerdo Ministerial Nro.14660; y publicado en el Registro Oficial Nro. 5, el 17 de agosto de 1992.
[15] Tomando en consideración que un Código de Ética no es, esencialmente, derecho, la aplicación del Código de Ética Médica en Ecuador constituye una norma, por la cual, se desprende principios generales que se aplican por los tribunales. Véase Gaceta Judicial. Año CIV. Serie XVII. Nro. 12. Página 3730; Resolución del Tribunal Constitucional Nro. 46, Registro Oficial Suplemento Nro. 66, 22 de abril de 2003; Expediente de Casación Nro. 94, Registro Oficial Suplemento Nro. 38, 5 de mayo de 2016; Expediente de Casación Nro. 79, Registro Oficial Nro. 87, 22 de mayo de 2003; Expediente de Casación Nro. 371, Registro Oficial Nro. 362, 23 de junio de 2004.
[16] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1099.

y porque, al fin y al cabo, este deber se presenta como uno de los pilares de la especial relación de confianza médico-paciente"[17].

Debe destacarse que la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de España –en adelante LOPDGDD–, precisa que los responsables y encargados del tratamiento de datos "así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad" –art. 5.1–. Tomando en consideración la norma que antecede, el RGPD recoge como un principio relativo al tratamiento de los datos personales a la integridad y confidencialidad, de tal manera que se garantice la seguridad de los datos y su protección contra el tratamiento no autorizado o ilícito.

Los datos relativos a la salud constituyen datos sensibles y, consecuentemente, pertenecen a una categoría de información más íntima de la persona. Así, "en el seno de esos datos ocupan un lugar relevante, hasta el punto de considerarse como informaciones especialmente sensibles, todos los datos que hacen referencia a la salud de cada persona"[18]. Dichos datos merecen una protección especial, ya que su tratamiento no autorizado o ilícito puede conducir a graves afectaciones de los derechos relacionados con la discriminación y el desarrollo de la personalidad. Por ello, este supuesto se relaciona con que los datos personales "no puedan ser conocidos por terceros, a excepción, claro está, de los supuestos que la legislación así lo establezca y, también evitar, que quienes están en contacto con los datos personales almacenados en los ficheros realicen filtraciones no consentidas de los mismos"[19]. En este sentido, el deber de secreto, de la reserva o deber de confidencialidad, se presenta como un principio fundamental en el tratamiento de la

[17] Andrea Casanova Asencio, "Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias", *Indret: Revista para el análisis del Derecho,* Nro. 1 (2019), 1-31.
[18] Enrique Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, (Madrid: Editorial Dykinson S.L, 2017), 172.
[19] María Nieves De la Serna Bilbao, "La protección de datos en el sector farmacéutico", en Jordi Faus Santasusana y José Vida Fernández (coord.), *Tratado de Derecho Farmacéutico. Estudio del régimen jurídico de los medicamentos*. España. Aranzadi. 2017.

información personal en el ámbito de la salud, caracterizado por el secreto profesional de quienes están vinculados con este sector[20].

Por consiguiente, advertimos que:

> Los datos de salud de un paciente son algo que afecta de lleno a la esfera más personal e íntima de una persona, algo que habitualmente puede querer reservarse para uno mismo o para los más cercanos. Su conocimiento por terceras personas puede atentar gravemente a la intimidad personal y familiar[21].

La importancia del secreto médico profesional en este contexto es fundamental, por cuanto como señala el Código de Ética "el interés público, la seguridad de los enfermos, la honra de las familias, la responsabilidad del profesional y la dignidad de la ciencia médica, exigen el secreto" –art. 66–. En este caso, señalamos que la Corte Constitucional de Ecuador –en adelante CCE–, en la Resolución 46 –Caso signado con el Nro. 46-2002-HD– sentó el siguiente criterio:

> Pues bien, analicemos lo que significa la tutela de los secretos frente a la divulgación dañina, y miremos al secreto profesional ya como aquella información que no puede ser revelada por recaer en los saberes o conocimientos relativos a la profesión o negocio que pueden ser aprovechados por la competencia desleal, los que no constituyen un bien con valor intrínseco, o la del secreto profesional relacionado con el deber que tienen los miembros de ciertas profesiones como el caso de los médicos de no descubrir a terceros los hechos que han conocido en el ejercicio de su profesión, como sería el caso de una enfermedad congénita, lesiones corporales, o del hecho de que una persona adolezca de SIDA, información que debe mantenerse secretamente, y que en estos casos sí afecta el derecho a la intimidad de las personas, a la honra y la buena reputación (…) En el caso que nos ocupa, el revelar datos estadísticos y la relación de los que han nacido en el Hospital Metropolitano los días 4, 5, 6, 7, 8 y 9 de mayo de 1987, no constituye develar un secreto connatural al ejercicio de la profesión del médico, que afecte al honor de las personas, por el contrario a través del *habeas data* que constituye una garantía constitucional en favor de las personas, se posibilita la obtención de información valiosísima que dará tranquilidad, sosiego y seguridad a la familia.

Esta resolución permite identificar la correlación de algunos bienes jurídicos en el derecho a la protección de datos personales. Es evidente que dentro del instituto de garantía que comprende este derecho existen otras libertades que deben ser tuteladas. Siendo así, "el limite al deber de secreto y, por tanto, al derecho a la intimidad del enfermo de sida se hace más patente para proteger el derecho a la

[20] Al respecto, la LOPDGDD determina que la obligación de guardar el deber de confidencialidad por parte de los responsables y encargados del tratamiento de datos "será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable" –art. 5.2–.
[21] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1102.

vida y a la salud de la persona con la que conviva"[22]. Si bien, la protección de los datos de carácter personal relativos a la salud tiene especial énfasis en la garantía de intimidad sobre el registro de la información que pertenecen a los pacientes, esta categoría de datos también tiene un alto valor económico para la comunidad científica. Sobre este aspecto, señalamos que:

> En el marco de la teoría de las libertades, ha surgido una tensión entre la exigencia de los poderes públicos de utilizar la transmisión de datos médicos, especialmente de los que hacen referencia a enfermedades contagiosas, o de aquellos que pueden ser utilizados para el desarrollo de avances en la investigación científica y el deseo de los ciudadanos de mantener una reserva sobre las informaciones que les conciernen[23].

Además, el Código de Ética establece que, excepcionalmente, "si por motivos científicos deben exhibirse o publicarse fotografías que permitan la identificación del paciente, se necesita autorización" –art. 73–. De esta manera, el consentimiento se concreta como uno de los principios que también requiere especial atención dentro del tratamiento de la información personal en el ámbito de la salud. Como señala la Guía Legislativa de la OEA, en el tratamiento de datos sensibles "el consentimiento explícito de la persona a la cual se refieran los datos debe ser la regla que rija la recopilación, la divulgación y el uso de datos personales sensibles"[24].

En todo caso, precisamos que en la protección de la información personal relativa a la salud, "no se trata de optar entre el derecho a la intimidad y una eficaz atención sanitaria sino buscar el respeto a todos ellos teniendo en cuenta el principio de proporcionalidad"[25]. Como bien señala la CCE, el deber de secreto o de confidencialidad tiene límites en cuanto existan bienes jurídicos constitucionales que deben ser ponderados al entrar en conflicto con otros derechos fundamentales.

### B. Ley Orgánica de la Salud

[22] Ibíd., 1178.
[23] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 172.
[24] Cfr. Guía Legislativa para los Estados Miembros de la OEA.
[25] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1104.

Otra norma relacionada con la protección de la información personal en este sector es la Ley Orgánica de la Salud[26]. Esta Ley describe el derecho a la salud como resultado de la construcción de ambientes, entornos y estilos saludables. Destaca que uno de los deberes del Estado es garantizar la intimidad de los pacientes. En este sentido, corresponde advertir que:

> La intimidad es un derecho que tiene por objeto el control de los datos personales que conciernen a los titulares de derechos fundamentales. En el seno de esos datos ocupan un lugar relevante, hasta el punto de considerarse como informaciones especialmente sensibles, todos los datos que hacen referencia a la salud de cada persona[27].

Así, la Ley Orgánica de la Salud reconoce que toda persona tiene el derecho al respeto de su dignidad, autonomía, privacidad e intimidad –art. 7.d)–. Naturalmente, esta garantía abarcaría la protección de los datos personales de los pacientes que –en calidad de información sensible– tutelaría la protección de este tipo de información.

Recordemos que, en el plano internacional, el RGPD reconoce como una categoría especial de datos personales a los datos relativos a la salud –art. 9.1–, en donde "la principal novedad es la inclusión de los datos genéticos y de los datos biométricos dentro de las categorías especiales de datos personales"[28]. Así, el RGPD define a los datos relativos a la salud como aquellos "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud" –art. 4.15–. Mientras que a los datos genéticos los define como "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa

[26] La Ley Orgánica de la Salud se aprobó, mediante Ley Nro.67 y fue publicado en el Registro Oficial Suplemento 423, el 22 de diciembre de 2006.
[27] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 172.
[28] Antonio Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada*, Nro. 49 (2018), 187-266.

persona, obtenidos en particular del análisis de una muestra biológica de tal persona" –art. 4.13–.

Destacamos que la legislación española, tanto en el ámbito estatal como autonómico, "ha prestado tradicionalmente una especial atención al derecho a la intimidad de los pacientes y de sus familiares. Hay que reconocer, por una parte, la especial vinculación entre las categorías especiales de datos personales y el derecho a la intimidad"[29]. Así, por ejemplo, la Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno prescribe que "cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos" –art. 5.3–, restringiendo también el ejercicio del derecho de acceso a la información pública cuando se solicite datos especialmente protegidos –art. 15.1–. En todo caso, la Ley General 33/2011 de Salud Pública reconoce a las personas el derecho "al respeto de su dignidad e intimidad personal y familiar en relación con su participación en actuaciones de salud pública" –art. 7.1–; y dispone que "la información personal que se emplee en las actuaciones de salud pública" se regirá según lo dispuesto por la LOPDGDD –art. 7.2–[30].

Ahora bien, la Ley Orgánica de la Salud de Ecuador reconoce el derecho a "tener una historia clínica única redactada en términos precisos, comprensibles y completos; así como la confidencialidad respecto de la información en ella contenida" –art. 7. f)–. En este orden, además, precisamos que el deber de confidencialidad implica la prohibición de divulgar a terceros la información personal

[29] Ibíd., 215.

[30] Hay que anotar que la Disposición Adicional Décimo Séptima de la LOPDGDD, sobre tratamientos de datos de salud, señala que "1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes Leyes y sus disposiciones de desarrollo: a) La Ley 14/1986, de 25 de abril, General de Sanidad. b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales. c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud. e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias. f) La Ley 14/2007, de 3 de julio, de Investigación biomédica. g) La Ley 33/2011, de 4 de octubre, General de Salud Pública. h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras. i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio. j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre".

que obra en una historia clínica. Por ello, también este deber comprende asegurar la confianza de los ciudadanos, mediante un entorno seguro y controlado. Así lo determina la Ley Orgánica de Protección de Datos en nuestro país –en adelante LOPD–, cuando exige que los responsables y encargados del tratamiento "estarán sujetos al deber de confidencialidad, de tal manera que se garantice una seguridad adecuada de los datos personales (…) mediante la aplicación de medidas técnicas organizativas apropiadas" –art. 30–. En todo caso, debemos advertir que "el mandato del deber de secreto que contiene la legislación obliga, no sólo al responsable del fichero sino también a todo aquel que intervenga en cualquier fase del tratamiento, dentro del cual también se incluye al encargado del tratamiento"[31].

Sobre esta cuestión, la Guía Legislativa de la OEA señala que uno de los presupuestos del derecho a la protección de datos "es el establecimiento y mantenimiento de la confianza entre el titular de los datos y el controlador de datos, especialmente con respecto a la divulgación de datos personales a terceros"[32]. En efecto, hoy en día el tratamiento de datos personales de los pacientes "ha sufrido un importante cambio con la aparición de las nuevas tecnologías informáticas, especialmente con la llegada de Internet, considerado, como es sabido, un medio global de intercambio y transmisión de todo tipo de información"[33]. Por tanto, "es importante ofrecer a los responsables de tratamientos de datos personales en el ámbito sanitario una certeza jurídica sobre cuáles son sus obligaciones y, sobre todo, cuáles son los derechos de las personas –de los pacientes–"[34].

Precisamente, la LOPD manifiesta que los datos relativos a la salud, tanto en el ámbito público como privado, "serán tratados cumpliendo los principios de confidencialidad y secreto profesional" –art. 31.1–; y siempre que sea posible,

[31] De la Serna Bilbao, "La protección de datos en el sector farmacéutico", en Jordi Faus Santasusana y José Vida Fernández (coord.).
[32] Cfr. Guía Legislativa para los Estados Miembros de la OEA.
[33] De la Serna Bilbao, "La protección de datos en el sector farmacéutico", en Jordi Faus Santasusana y José Vida Fernández (coord.).
[34] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 194.

"deberán ser previamente anonimizados o seudonimizados, evitando la posibilidad de identificar a los titulares de los mismos" –art. 31.2–. A la luz del RGPD, conviene advertir que "no parece aquí muy atinado el precepto pues la anonimización es definitiva en cuanto a la imposibilidad de reidentificar al sujeto cuyos datos se han anonimizado (de hecho, los datos anonimizados son irrelevantes a efectos de la aplicación de las leyes de protección de datos)"[35].

Por otra parte, como una garantía de confianza o certeza, el derecho a la protección de datos plantea la observancia del consentimiento. El ordenamiento constitucional ecuatoriano reconoce que los servicios de salud "garantizarán el consentimiento informado, el acceso a la información y la confidencialidad de la información de los pacientes" –art. 362–[36]. No obstante, el tratamiento de la información que obra en una historia clínica es una de las cuestiones que presenta varios conflictos en la materia. Precisamente, "las dudas sobre la titularidad de la historia clínica y los distintos niveles de acceso ha favorecido la aparición de frecuentes conflictos que han terminado en el ámbito jurisdiccional"[37]. Desde esta perspectiva, la LOPD plantea dos excepciones, sobre el consentimiento del titular, para el tratamiento de datos. La primera, "cuando sea necesario por razones de interés público esencial" y, la segunda, "en el caso de amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios" –art. 30–. Todo ello está, naturalmente, vinculado a la adopción de medidas adecuadas y específicas, que garanticen los derechos de los titulares.

Dentro del conjunto de derechos que se atribuyen a las personas en relación a la salud, la Ley Orgánica de la Salud, expresamente, no hace referencia al ejercicio

[35] María Mercedes Serrano Pérez, "El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del Reglamento General de Protección de Datos y de la Ley de Protección de Datos Personales y garantía de los derechos", *Estudios de Deusto. Revista de la Universidad de Deusto*, Nro. 2 (2020), 257-292.
[36] Tómese en cuenta que, "el derecho a la protección de datos era calificado, desde una perspectiva doctrinal, como un derecho a la autodeterminación informativa, una expresión que manifestaba la importancia del consentimiento individual". Cfr. Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 218.
[37] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1115.

de los derechos de acceso, rectificación, cancelación y oposición como una fórmula para garantizar el control de la información personal. Sin embargo, esta Ley reconoce el derecho a “utilizar con oportunidad y eficacia, en las instancias competentes, las acciones para tramitar quejas y reclamos administrativos o judiciales que garanticen el cumplimiento de sus derechos” –art. 7. f)–. En todo caso, la LOPD es clara al precisar que el titular podrá, en cualquier momento, “presentar requerimientos, peticiones, quejas o reclamaciones directamente al responsable del tratamiento, relacionadas con el ejercicio de sus derechos “–art. 62–.

En el caso ecuatoriano, la garantía del derecho a la protección de datos, en el ámbito de la salud, tiene algunos presupuestos pendientes. Si bien existen prescripciones, en el marco de la LOPD; es evidente la falta de normativa vinculada a establecer mecanismos de seguridad y criterios de confianza respecto al tratamiento de la información sensible; y sobre todo la necesidad de aclarar los mecanismos que garanticen el control y dominio que sobre aquella recae.

Finalmente, la jurisprudencia de la CCE ha incidido en el desarrollo de los derechos que se desprenden del tratamiento de la información personal en el sector de la salud. Por ejemplo, la Resolución 16 –Caso signado con el Nro. 2014-12-EP–, acogiendo el criterio de la Corte Interamericana de Derechos Humanos y del Comité de Derechos Económicos, Sociales y Culturales de Naciones Unidas, apunta que:

> La Corte Interamericana de Derechos Humanos en el caso Gonzales Lluy y otros vs. Ecuador estableció que: *En el marco de este corpus iuris en la materia, la Corte considera que el VIH es un motivo por el cual está prohibida la discriminación en el marco del término "otra condición social" establecido en el artículo 1.1 de la Convención Americana*. En esta protección contra la discriminación bajo "otra condición social" se encuentra asimismo la condición de persona con VIH con aspecto potencialmente generador de discapacidad en aquellos casos donde, además de las afectaciones orgánicas emanadas del VIH, existan barreras económicas sociales o de otra índole derivadas del VIH que afecten su desarrollo y participación en la sociedad (…) En consecuencia, *los jueces constitucionales al reducir derechos de elemental importancia como lo es el derecho a la salud que se encuentra relacionado directamente con otros derechos como el de la vida, integridad personal y dignidad humana, no solo generan una desprotección constitucional, sino que además generan una violación directa contra estos derechos, lo cual se constituye en una actuación inconcebible dentro del modelo constitucional vigente en el Ecuador a partir de la expedición de la Constitución del 2008*. En el caso concreto, se evidencia que la autoridad judicial emite criterios que no solo dejan en desprotección al accionante, al no pronunciarse sobre la falta de atención médica en razón de su enfermedad, sino que además vulneran sus derechos constitucionales puesto que la jueza concibe a las personas portadoras de VIH o enfermas

> de SIDA, como aquellas que deben buscar la forma de adaptarse a la sociedad; es decir, *la autoridad judicial desconoce la igualdad material prevista en la Constitución y lo señalado en la jurisprudencia expedida por la Corte Interamericana de Derechos Humanos, la cual no solo incluye que todas las personas sean tratadas como iguales ante la Ley, sino que además las personas que se encuentra en una situación diferente sean tratadas en función de esta diferencia, a efectos de alcanzar la igualdad material y no incurrir en una discriminación de sus derechos*. Por su parte, el Comité de Derechos Económicos, Sociales y Culturales de Naciones Unidas en su Observación General Nro. 14 determinó que el derecho a la salud presenta cuatro elementos esenciales e interrelacionados: disponibilidad, accesibilidad, aceptabilidad y calidad (…) Como tercer elemento del derecho a la salud, aparece la aceptabilidad por la cual: *Todos los establecimientos, bienes y servicios de salud deberán ser respetuosos de la ética médica y culturalmente apropiados, es decir respetuosos de la cultura de las personas, las minorías, los pueblos y las comunidades, a la par que sensibles a los requisitos del género y el ciclo de vida, y deberán estar concebidos para respetar la confidencialidad y mejorar el estado de salud de las personas de que se trate*.

La misma resolución, respecto al deber de protección integral del derecho a la salud por el Estado, resalta la importancia de evitar intromisiones de terceros. En este aspecto, se destaca que:

> El accionar del Estado para la defensa de los derechos se efectúa a través de estas tres garantías: la de prestación cuando permite su accesibilidad; la de abstención, cuando el Estado se inhibe de efectuar algún acto que pueda menoscabar los derechos a través de la garantía de respeto, y *la de protección, cuando garantiza la no intromisión de terceros en el ejercicio de los derechos, sin dejar de lado las garantías constitucionales cuyo objetivo es viabilizar la efectividad de los derechos a través de la justiciabilidad de estos, cuando hayan sido vulnerados. Por lo que se dispone que las autoridades pertinentes del Ministerio del Interior y de la Policía Nacional, asegurando y preservando el derecho a la intimidad y buen nombre de las personas, inicien un proceso de evaluación médica reservado para identificar a los miembros de la institución que padezcan esta enfermedad y otras enfermedades catastróficas*, y definan acciones administrativas, presupuestarias y médicas para atender de forma prioritaria los requerimientos de los miembros de la institución que sean portadoras de VIH o enfermos de SIDA, o que se encuentren en situaciones de enfermedades catastróficas análogas.

Debemos recalcar que el desarrollo legislativo de los derechos relacionados a la autodeterminación informativa en la salud es aún deficiente. De ahí que, la jurisprudencia también ha sido escasa en poder determinar los límites que conlleva asignar la protección de este derecho. A esto se suman dos problemas recurrentes en la actualidad. Primero, la falta de conocimiento respecto al alcance que tiene el derecho a la protección de datos en el sector de la salud; y segundo, el desinterés de los legisladores en advertir la existencia de “nuevos riesgos sobre el derecho fundamental a la protección de datos personales que provienen de tratamientos de datos personales en el ámbito sanitario como la generalización de la historia clínica

electrónica"[38]. Urgen reformas relativas a la protección de datos genéticos, que –como una categoría especial en los datos relativos a la salud– exigen mecanismos adecuados de protección en el tratamiento de información de carácter sensible. En todo caso, la LOPD –que articula principios y garantiza mecanismos de seguridad, disociación, control y dominio de la información personal– será fundamental, al momento de armonizar la legislación sectorial en el ámbito de la salud. Todo ello, sin perjuicio de que el derecho a la protección de datos deba presentar excepciones en el ámbito de la salud para garantizar la asistencia, la salud pública y la investigación sanitaria[39].

### 2.2 La protección de datos personales en el Sector Social

#### A. Ley de Seguridad Social

De manera preliminar, nos gustaría aclarar que el RGPD establece que la legislación de protección de datos aplicable a los responsables o encargados del tratamiento, podrá limitar el alcance de los derechos y las obligaciones que se desprenden del derecho fundamental a la protección de datos personales. Así, en el ámbito de la seguridad social, el RGPD señala excepciones, siempre y cuando

[38] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 252.

[39] Así, por ejemplo, advertimos que el RGPD "está llamando al legislador de los Estados miembros para que concrete las garantías y las excepciones de los derechos en estos tratamientos (…) específicamente el art. 9.2.h), i) y j) del RGPD regula que los tratamientos con fines de asistencia sanitaria, salud pública e investigación sanitaria pueden llevarse a cabo con categorías especiales siempre sobre la base no sólo del Derecho de la Unión sino también del Derecho de los Estados miembros. De hecho, le corresponde al Derecho de la Unión o de los Estados miembros establecer para los tratamientos por razones de interés público en el ámbito de la salud, medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional –art. 9.2.i) RGPD–. En todo caso, le corresponde no sólo al Derecho de la Unión sino también al Derecho de los Estados miembros establecer las obligaciones de secreto profesional para los tratamientos de datos para la asistencia sanitaria –art. 9.3 RGPD–. Finalmente, el Derecho de los Estados miembros y no sólo el Derecho de la Unión puede establecer las excepciones a los derechos para los tratamientos de categorías especiales de datos personales con finalidad de investigación, siempre que estos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuando esas excepciones sean necesarias para alcanzar estos fines –art. 89.2 RGPD–". Cfr. Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 252.

se “respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada” –art. 23.1. e)–[40]. Por ejemplo, el RGPD prescribe que la prohibición no será de aplicación cuando “el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social” –art. 9.2. b)–. Por tanto, este supuesto “se aplica a los tratamientos de categorías especiales de datos en el ámbito de la seguridad social y de los servicios sociales”[41].

El tratamiento excepcional de datos personales en el sector de la seguridad social y de los servicios sociales exige que sea una medida necesaria y proporcionada, que respete, esencialmente, los derechos y libertades fundamentales. Por ello, como describe la Guía Legislativa de la OEA, “la protección efectiva de los derechos individuales de protección de la privacidad y de los datos se basa tanto en la conducta responsable de los controladores de datos como en las personas y en las autoridades gubernamentales del caso”. Así, advertimos que “la actividad social de los poderes públicos, animada por indudables principios éticos, tiene que estar orientada también a salvaguardar el derecho a la intimidad y a la confidencialidad de la información personal”[42].

En el marco de la legislación ecuatoriana el seguro general obligatorio, que forma parte del sistema nacional de seguridad social, se regula, mediante las

[40] El RGPD aclara que “deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos” –Considerando 52–.

[41] Troncoso, “Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales”, 233.

[42] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1364**.**

disposiciones de la Ley de Seguridad Social[43]. El objeto de esta Ley se orienta a proteger los derechos de "todas las personas que perciben ingresos por la ejecución de una obra o la prestación de un servicio físico o intelectual, con relación laboral o sin ella" –art. 2–. Desde esta perspectiva, el art. 247 de la Ley de Seguridad Social determina que:

> En la forma, dentro de los plazos, y con una periodicidad no mayor de un año, el IESS deberá remitir al asegurado la información contenida en su respectivo Registro de Historia Laboral, sin perjuicio del derecho que asiste al asegurado para solicitar, en cualquier momento dicha información. El incumplimiento de esta obligación de informar al asegurado constituye un acto administrativo susceptible de sanción y apelación, de acuerdo con las disposiciones de esta Ley. La información de la historia laboral del asegurado es reservada. El quebrantamiento de la prohibición de revelar los datos contenidos en ella será sancionado con arreglo al Código Penal. Sin perjuicio de lo dispuesto en el inciso anterior, la información de la historia laboral podrá darse a conocer de conformidad con la Ley, a los tribunales y jueces competentes, así como a petición del afiliado, o si éste hubiere fallecido a solicitud de las personas que tuvieren derecho a pensiones de viudez y orfandad.

Corresponde aclarar que la historia laboral se asemeja a lo que en otros sistemas jurídicos se consideran como una historia social. Constituye un instrumento en el cual "se registran exhaustivamente los datos personales, familiares, sanitarios, de vivienda, económicos, laborales, educativos y cualesquiera otros significativos de la situación socio-familiar de un usuario, la demanda, el diagnóstico y la subsiguiente intervención y la evolución de su situación personal"[44]. De esta manera, es evidente que la historia laboral o social contiene información reservada a los intereses del titular de los datos personales y que puede representar una fuente de valor económico para terceras personas.

[43] La Ley de Seguridad Social se aprobó, a través de la Ley Nro.55 y fue publicada en el Registro Oficial Nro. 465, el 30 de agosto de 2001. Esta Ley determina que el Seguro General Obligatorio se fundamenta en los principios de solidaridad, obligatoriedad, universalidad, equidad, eficiencia, subsidiariedad y suficiencia.

[44] La definición de historia social se encuentra definida conforme en lo dispuesto por el art. 3 del Código Deontológico de los Trabajadores Sociales de España. Cfr. Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1365. Sobre esta base, asociamos a la historia laboral, a partir de lo dispuesto en la Ley de Seguridad Social, la cual señala: "El Registro de Historia Laboral del Asegurado comprenderá la siguiente información: a. Datos personales del asegurado; b. Datos de los familiares dependientes del asegurado; c. Fecha de ingreso al Seguro General Obligatorio; d. Tiempo de servicios, remuneración imponible y aportes pagados por cada empleador, que serán declarados por éste o por iniciativa del propio afiliado o por comprobación del IESS, de conformidad con las reglas de aplicación de este Título; y e. En el caso del asegurado sin empleador, aquellos servicios y remuneraciones imponibles por los que haya cotizado o cotizare, dentro de los límites que establecerá la reglamentación" –art. 244–.

La interpretación de la norma que antecede contiene, no solamente una referencia al deber de confidencialidad, reserva o secreto de la información, sino que, también se remite al principio de responsabilidad, frente al tratamiento de la información personal. Para el cumplimiento de este principio, es fundamental la actividad que desarrollan los encargados y responsables del tratamiento. Al respecto, la Guía Legislativa de la OEA recomienda que, para garantizar el principio de responsabilidad, las Leyes y normas sectoriales deben establecer medidas apropiadas que se orienten a proteger la intimidad y carácter reservado de la información. Por ejemplo, la Guía de la OEA advierte la necesidad de "impulsar la elaboración de códigos de conducta autónomos que se mantengan a la par de los adelantos tecnológicos y que tengan en cuenta los principios y normas de privacidad vigentes en otras jurisdicciones"[45].

En el texto del art. 247 de la Ley de Seguridad Social encontramos cuatro precisiones importantes. La primera relacionada al derecho de acceso de la información personal contenida en la bases de datos del Instituto Ecuatoriano de Seguridad Social; la segunda encaminada a que el derecho de acceso se garantice por medio de sanciones administrativas, para el supuesto en que el funcionario que posee la información lo negare; la tercera vinculada a los principios o deber de secreto y responsabilidad en el tratamiento de los datos personales; y la cuarta referida a la excepcionalidad del sigilo de la información, cuando la Ley o la autoridad competente ordene su levantamiento.

Es conveniente precisar que, el tratamiento de la información personal en el sector social, "tiene que respetar también los derechos de las personas en este ámbito, entre los que se destacan los derechos de acceso, rectificación y cancelación sobre sus propios datos"[46]. Así, advertimos que esta Ley reconoce el ejercicio del derecho de rectificación sobre las informaciones relativas al trabajador, por el cual se

[45] Asimismo, para garantizar el cumplimiento de este principio, la Guía Legislativa de la OEA determina que: "en las Leyes nacionales sobre privacidad se debe exigir que los controladores de datos rindan cuenta del cumplimiento de estos principios. Además del mecanismo con que cuenten las autoridades gubernamentales para hacer cumplir la normativa, el derecho interno debe proveer a las personas de mecanismos apropiados para responsabilizar a los controladores de datos de las violaciones que se produzcan (por ejemplo, mediante la indemnización por daños y perjuicios)".
[46] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1401.

garantiza el derecho a la observación de la información, señalando que "el asegurado podrá consignar sus observaciones para la correspondiente rectificación, sujeta a la comprobación de la veracidad por parte del IESS" –art. 248–.

Si bien en la Ley de Seguridad Social, no existen otras disposiciones relacionadas con la garantía de control sobre el tratamiento de la información, la CCE sentó un trascendental precedente, específicamente, en el ámbito de la seguridad social, señalando que toda persona tiene derecho a "ejercer su derecho de actualizar, rectificar, eliminar o anular dicha información, con la finalidad de que tenga, en algún grado, control sobre el uso que se dé a la información personal"[47]. Esta resolución puede considerarse como una de las más completas, por cuanto se pronuncia sobre el contenido del derecho a la protección de datos y su tutela en el servicio público.

Así, sobre las facultades que se desprenden del *habeas data,* la Corte señala que:

> Esta garantía tiene como finalidad el acceso a los documentos, bancos o archivos referentes a la persona solicitante que consten en entidades públicas o privadas, así como en caso de que la información proporcionada resulte falsa, errónea, antigua, incierta, obsoleta, discriminatoria o inexacta, exigir su actualización, rectificación, eliminación, anulación o confidencialidad. En este sentido, el texto constitucional consagra al *habeas data* como un derecho fundamental en sí mismo, independiente de otros y como un mecanismo de protección de otros derechos fundamentales, como el derecho a la honra, al honor, a la intimidad, al buen nombre, a la imagen, a la verdad, al patrimonio, a la privacidad, a la voz y a la autodeterminación informativa frente al abuso y negligencia en el tratamiento de la información.

En referencia a los principios relativos al tratamiento de la información, la CCE precisa que:

> Otro aspecto importante es el principio de utilidad, bajo el cual, la información constante en documentos, datos genéticos, bancos o archivos de datos, que reposa en entidades públicas o privadas, en soporte material o electrónico, debe cumplir una función específica, que implica la satisfacción de un interés legítimo determinado por la importancia y utilidad de la información (…) A ello va ligado, entonces, la responsabilidad de la entidad pública, llámese Instituto Ecuatoriano de Seguridad Social, IESS, de administrar la información en una base de datos confiable, que responda a principios de necesidad, veracidad, integridad, finalidad, utilidad, entre otros, puesto que la información que difunda debe ser veraz e imparcial, y sobre todo no puede vulnerar derechos fundamentales de los afiliados. Por la importancia de la información que manejan respecto a cada uno de los afiliados o asegurados, corresponde también un manejo responsable de la misma, debido a que cualquier acción u omisión en su tratamiento por parte de los servidores públicos responsables puede generar una violación a derechos fundamentales de las personas, como en el presente caso. No podemos permitir que la negligencia o dolo de los servidores públicos llamados a

[47] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-09-SEP-CC (CASO Nro. 14-09-EP) publicada en el Registro Oficial 18 de 03-sep.-2009.

> desempeñar su trabajo con eficiencia y responsabilidad lesione gravemente derechos fundamentales de las personas, en este caso, de los afiliados.

Como habíamos señalado, inicialmente, por disposición constitucional prevista en el art. 11.8, el contenido de los derechos fundamentales conlleva que se desarrollen de manera progresiva, mediante políticas públicas que garanticen en la Administración Pública condiciones necesarias para su pleno reconocimiento y ejercicio. Sobre esta cuestión, la CCE refiere que:

> Es obligación de las entidades públicas o privadas que se encargan de la recolección, manejo, archivo y circulación de información en documentos, informes, datos genéticos, bancos o archivos de datos, garantizar a las personas que la información que se recoja sea actualizada en forma permanente. Adicionalmente, es reprochable la conducta negligente por parte del Instituto Ecuatoriano de Seguridad Social, al no obrar con el cuidado y diligencia que le impone la responsabilidad constitucional de prestar el servicio de seguridad social, al no contar con un archivo que custodie la información de cada uno de los afiliados en el país en forma adecuada (…) En este orden de ideas, cabe señalar que las instituciones públicas, garantes de la Constitución de la República, están obligadas, en lo que respecta al manejo de información, a velar por la exactitud y fidelidad de los datos registrados, sea en medio manual o informático, por la legalidad en su recolección, por el seguimiento y su constante actualización, por la implementación de dispositivos que impidan accesos no autorizados, entre otros (…) Esta serie de conductas y prácticas llevadas a cabo por el IESS en el manejo de la información son consideradas indebidas e ilegítimas, atentatorias al efectivo goce de los derechos fundamentales y contrarias a las acciones que debe desplegar el Estado con el fin de lograr dar cumplimiento a sus deberes primordiales, como el de garantizar, sin discriminación alguna, el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales.

Según estas apreciaciones, es una de las resoluciones que mejor ha desarrollado los criterios de responsabilidad en el tratamiento de la información personal, en la Administración Pública, por cuanto la CCE precisa que el respeto del derecho a la protección de datos, no constituye, solamente, un deber contemplado en la Constitución, sino que, también conlleva una serie de procedimientos, que deben ser observados por los responsables del tratamiento de la información.

A partir del deber de secreto o confidencialidad, la Ley de Seguridad Social y la CCE destacan el alcance del principio de responsabilidad en el tratamiento de la información, señalando que este principio implica la implementación de medidas de seguridad –principio de seguridad de datos– para el cumplimiento de los principios de secreto o confidencialidad. Por una parte, se hace referencia a la previsión del principio de calidad de datos, bajo el cual la información –que obra en poder de la Administración Pública– debe sujetarse a ciertas condiciones relacionadas con el respeto de la finalidad, pertinencia y proporcionalidad en la recogida de datos. Y por

otra parte, al principio de seguridad de los datos, puesto que el responsable y/o encargado del tratamiento debe adoptar las medidas necesarias para la seguridad de la información personal.

Hay que subrayar que, en la Ley de Seguridad Social, no solo hacen falta previsiones respecto a las limitaciones o excepciones que comporta el tratamiento de la información. También se desprende la necesidad de medidas –principio de seguridad de datos– que los encargados o responsables deben adoptar para asegurar que el tratamiento cumpla con los principios de finalidad, pertinencia y proporcionalidad[48]. Lógicamente, como analizaremos en otro momento, estas cuestiones se encuentran reguladas en la LOPD. En todo caso, debe existir especial atención sobre el principio de calidad de datos en los servicios sociales, por cuanto comprende "racionalizar los datos personales que se recaban de los ciudadanos, sobre todo aquellos datos especialmente protegidos, tratando únicamente los datos adecuados y pertinentes –a pesar de haber sido aportados voluntariamente por el interesado– y aplicando el principio de proporcionalidad"[49]. Por ello, como señala la CCE, particular significación tiene el principio de utilidad –finalidad– en el tratamiento de la información, toda vez, que ésta debe ser utilizada o destinada para los fines bajo los cuales fue recabada.

Conviene insistir, entonces, en que la LOPD será la que determine los principios que deben observarse, dentro del tratamiento de la información de las personas sometidas al régimen de la Ley de Seguridad Social. Además, de precisar las obligaciones y responsabilidades de los encargados del tratamiento, ya que este derecho –debido a su importancia y su correlación con otras libertades fundamentales– , exige que la Administración Pública genere y garantice las condiciones necesarias para su pleno reconocimiento y ejercicio. Naturalmente,

[48] Como señala la Guía Legislativa de la OEA, se debe "adoptar programas efectivos de gestión de la privacidad y realizar revisiones internas con el propósito de promover la privacidad de las personas. En muchos casos, la designación de un "responsable principal de la información y la privacidad" facilitará la consecución de esta meta".
[49] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1374, 1375.

también será necesario establecer –bien en esta normativa sectorial o en el reglamento de la LOPD– que las excepciones a los tratamientos de datos en el ámbito seguridad social y de los servicios sociales sean una medida necesaria y proporcionada, caracterizada por el respeto de los derechos y libertades fundamentales.

### B. Código de la Niñez y la Adolescencia

La protección de datos personales en el Código de la Niñez y la Adolescencia –en adelante CNA– se enmarca en el principio del derecho internacional reconocido como "interés superior del menor"[50]. En el marco constitucional, este principio satisface, desde el ámbito jurídico y social el ejercicio efectivo de los derechos de los niños, niñas y adolescentes –art. 44–[51]. En materia de protección de datos, el interés superior del menor plantea que "se proteja la intimidad del niño del mejor modo posible, dando efecto en la mayor medida posible a los derechos de protección de datos del niño"[52].

En la Constitución, la niñez y la adolescencia se consideran como un grupo de atención prioritaria –art. 35–, bajo el cual gozan de los derechos comunes del ser humano, reconociéndose y garantizándose el respeto de su libertad y dignidad –art. 45–. Así, considerando que el derecho a la protección de datos se encuentra reconocido como un derecho de libertad, cuya tutela se asienta sobre la base de la dignidad humana; en el caso de la niñez y la adolescencia este derecho precisa una

[50] El Código de la Niñez y la Adolescencia se aprobó, mediante la Ley Nro.100 y fue publicada en el Registro Oficial 737 el 3 de enero de 2003.
[51] Como señala la CCE, "la frase del artículo 44 "se atenderá al principio de su interés superior y sus derechos prevalecerán sobre los de las demás personas...", interpretada en su integralidad e interconexión es un principio rector-guía, en los términos que ha desarrollado esta Corte, una garantía social que obliga al Estado a una actuación concreta y efectiva para garantizar los derechos de niñas, niños y adolescentes, y a la vez, es un principio constitucional directamente aplicable y justiciable, pero en igualdad con otros principios y derechos de acuerdo a lo que establece el artículo 11 numeral 6 de la Constitución vigente". Cfr. la Resolución 10 (Caso signado con el Nro. 1277-10-EP) de la Corte Constitucional para el período de transición.
[52] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 187.

máxima protección, ya que, en el aseguramiento del ejercicio de sus derechos, se atenderá siguiendo el principio de interés superior del menor.

Como precisa la Guía Legislativa de la OEA "los menores (personas que no han llegado a la edad adulta) también tienen intereses legítimos en materia de privacidad que deben reconocerse y protegerse efectivamente en la legislación nacional". En este contexto, el CNA garantiza la protección de datos personales, mediante el respeto del derecho a la intimidad de su vida privada y familiar; al derecho a la privacidad de su correspondencia y comunicaciones telefónicas o electrónicas –art. 53–[53]. En todo caso, atendiendo las disposiciones de la LOPD, debe considerarse que los datos relativos a la niñez y la adolescencia se encuentran incluidos dentro de las categorías que merecen una especial protección –art. 25.b)–.

En este orden, conforme en lo dispuesto en el art. 8 del CNA, la protección de la intimidad y de los datos personales de la niñez y la adolescencia se afirma, además, en el principio de corresponsabilidad, por el cual se establece –como un deber del Estado, la sociedad y la familia– "adoptar las medidas políticas, administrativas, económicas, legislativas, sociales y jurídicas que sean necesarias para la plena vigencia, ejercicio efectivo, garantía, protección y exigibilidad de la totalidad de los derechos de niños; niñas y adolescentes"[54]. Sin perjuicio de lo señalado, "no huelga advertir, que el respeto del derecho a la intimidad debe ser promovido también en lo que afecta a la relación de los niños con otros niños"[55].

[53] En este aspecto, el CND señala que "sin perjuicio de la natural vigilancia de los padres y maestros, los niños, niñas y adolescentes tienen derecho a que se respete la intimidad de su vida privada y familiar; y la privacidad e inviolabilidad de su domicilio, correspondencia y comunicaciones telefónicas y electrónicas, de conformidad con la Ley. Se prohíbe las injerencias arbitrarias o ilegales en su vida privada" –art. 53–.

[54] Incluso, el deber de corresponsabilidad en la protección y garantía de los derechos relativos a la niñez y la adolescencia constituye un deber constitucional, que obliga a "asistir, alimentar, educar y cuidar a las hijas e hijos. Este deber es corresponsabilidad de madres y padres en igual proporción, y corresponderá también a las hijas e hijos cuando las madres y padres lo necesiten" –art. 83.16–. En todo caso, para proteger los derechos de las personas integrantes de la familia, el Estado "promoverá la corresponsabilidad materna y paterna y vigilará el cumplimiento de los deberes y derechos recíprocos entre madres, padres, hijas e hijos" –art. 69.5–.

[55] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 186.

El Estado está obligado a una actuación concreta y efectiva, que garantice el derecho a la protección de datos y, en lo que respecta a la sociedad y la familia, corresponde una tutela integral que garantice a los menores sus intereses legítimos en materia de privacidad, en la sociedad de la información. Sobre este planteamiento, recordemos que la LOPDGDD contiene nuevos preceptos relacionados con la garantía de los derechos digitales. Por ejemplo, se determina que los padres, madres, tutores, curadores o representantes legales procuren que los menores "hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales" –art. 84.1–[56]. Precisamente, advertimos que la LOPD prescribe que, a la luz del concepto de corresponsabilidad debe garantizarse la construcción de un espacio "seguro y responsable de las tecnologías de la información y comunicación, en estricto apego a la dignidad e integridad humana, los derechos fundamentales y libertades individuales" –art. 23–.

Por otra parte, hemos señalado que la información de carácter personal de la niñez y la adolescencia constituyen datos especialmente protegidos, que en su tratamiento pueden acarrear discriminación. Así, frente al desconocimiento de los riesgos que supone compartir datos personales en Internet y redes sociales, aclaramos que dicha información "publicada por un usuario en su página personal no sólo permite fácilmente establecer un perfil personal, sino que incluye, en muchas ocasiones, datos sobre vida sexual, ideologías, religión, que es una información considerada por la normativa como de especial protección"[57].

En este caso, hay que apuntar que la Constitución –como un principio de aplicación de los derechos– reconoce que ninguna persona será discriminada "por razones de etnia, lugar de nacimiento, edad, sexo, identidad de género, identidad cultural,

[56] Además, hay que destacar que el art. 83 de la LOPDGDD reconoce el derecho a la educación digital –que enmarca, por ejemplo, el respeto de la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales– bajo el cual el sistema educativo debe garantizar las actuación y participación de la administración educativa, alumnado, profesorado.
[57] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1693.

estado civil, idioma, religión, ideología, filiación política, pasado judicial, condición socio-económica, condición migratoria, orientación sexual, estado de salud, portar VIH, discapacidad, diferencia física" –art. 11.2–. Además, el CNA refiere a la no discriminación como un principio básico para el ejercicio de los derechos de los menores, por el cual no podrán ser discriminados por causas de "su nacimiento, nacionalidad, edad, sexo, etnia; color, origen social, idioma, religión, filiación, opinión política, situación económica, orientación sexual, estado de salud, discapacidad o diversidad cultural o cualquier otra condición propia o de sus progenitores, representantes o familiares" –art. 6–.

Entre las medidas que aseguren el pleno ejercicio de estos derechos, la Constitución exige que el Estado deberá adoptar mecanismos de protección, frente a la influencia de programas o mensajes que promuevan toda forma de discriminación –art. 46.7–[58]. Lógicamente, dichas mecanismos de protección no corresponden, únicamente, al Estado sino también a toda la sociedad, incluida la familia. Por ello, consideramos que "urge promover una *Paideia*, es decir, una educación y cultura cívica en los menores para garantizar la consciencia del valor de la intimidad como un bien jurídico que debe ser respetado en ellos y en todos los demás"[59]. Sin duda, tomando en cuenta la LOPD, se trata de un presupuesto que deberá respetarse, por cuanto dicha Ley caracteriza la necesidad de "promover una cultura sensibilizada en el derecho de protección de datos personales" –art. 23–.

Con referencia a lo que se acaba de señalar, la Resolución 30 (Caso signado con el Nro. 30-2006-TC) de la CCE que declaró la inconstitucionalidad parcial del artículo 2, letra a) de la Ley de Maternidad Gratuita, señala que:

> A criterio de los actores la frase "excepto SIDA" impugnada es inconstitucional por contrariar el derecho a la igualdad y a la prohibición de no discriminación (…) De la revisión de la Ley para la Prevención y Asistencia Integral del VIH/SIDA no se encuentra disposición alguna que de manera expresa derogue la frase "excepto SIDA" contenida en la letra a) del artículo

[58] Por ejemplo, la LOPDGDD determina que "la utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor" –art. 84.2–.

[59] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 186.

> 2 de la Ley de Maternidad Gratuita (…) el artículo de la Ley para la Prevención y Asistencia Integral del VIH/SIDA declara de interés nacional la lucha contra el sida, dispone el fortalecimiento de la prevención de la enfermedad, garantiza vigilancia epidemiológica y facilita el tratamiento a personas afectadas, asegura el diagnóstico en bancos de sangre y laboratorios precautela los derechos, respeto, no marginación y confidencialidad de datos (…) Las palabras "excepto SIDA" contenidas en la Ley de Maternidad Gratuita cuya declaratoria de inconstitucionalidad se demanda, determinan que las mujeres afectadas con VIH/sida que se encuentran en estado de gestación, durante el parto y en el posparto no sean beneficiarias de la atención de salud gratuita y de calidad que como derecho económico social y cultural ha sido reconocido en la referida Ley. En consecuencia, no solo por disposición constitucional sino también por así disponer instrumentos internacionales sobre derechos humanos suscritos y ratificados por el Ecuador, el Estado se obliga a garantizar la igualdad de las personas ante la Ley y su no discriminación, por tanto, la frase "excepto Sida" impugnada, contraría el derecho consagrado en los artículos 23, número 3 y 47 de la Constitución Política, 24 de la Convención Americana de Derechos Humanos y 26 del Paco Internacional de Derechos Civiles y Políticos que es parte de nuestro ordenamiento jurídico por así disponerlo el artículo 163 de la Carta Política.

Según lo expuesto por la CCE y considerando que “el derecho a la protección de datos personales, es como hemos señalado antes, un derecho personalísimo por lo que por regla general debe poder ser ejercido por los menores”[60]; advertimos que este derecho faculta exigir de los poderes públicos la erradicación de elementos discriminatorios que se desprenden del tratamiento de datos personales. Además, debe considerarse que “los niños, por ser menores de edad, tienen limitada su capacidad de obrar. Por tal motivo muchas de sus actuaciones deben ser realizadas por quienes ostentan su representación legal”[61].

Del análisis del CNA, evidenciamos la ausencia de disposiciones relativas al ejercicio de los derechos de control de la información personal; sobre la prestación del consentimiento para el tratamiento de datos; y en todo caso, sobre las reglas de quién ejerce la representación para el ejercicio de este derecho fundamental, hasta que los menores alcancen la mayoría de edad. Así también, conforme prescribe el RGPD, “dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender” –Considerando 58–; enfatizamos en la necesidad de prever mecanismos que aseguren el principio de transparencia, frente a los menores.

[60] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1229**.**
[61] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 186.

De la misma manera, en el sistema educativo insistimos en la necesidad de formular garantías relacionadas con el uso responsable de las tecnologías de la información y comunicación, las cuales propendan al respeto de la dignidad humana, intimidad y protección de datos en entornos digitales. Por último, recalcamos en que dichas previsiones se encuentran reconocidas en la LOPD, pero que, complementariamente, deben desarrollarse en la normativa del CNA. Naturalmente, sobre la base de los principios de corresponsabilidad y de interés superior del menor, la nueva normativa de protección de datos pretende concretar los criterios, bajo los cuales deban efectuarse los tratamientos de datos personales de la niñez y la adolescencia.

## 2.3 La protección de datos personales en el Comercio Electrónico

### A. Ley de Comercio Electrónico, Firmas y Mensajes de Datos

Una de las principales características, que ha impulsado el desarrollo del derecho a la protección de datos personales, ha sido la evolución de la tecnología. Este derecho, destinado a proteger la libertad informática, se encuentra también regulado en la normativa de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos[62]. Considerando que "el derecho fundamental a la protección de datos personales no trata de impedir el recurso a las nuevas tecnologías sino de conciliarlo con el respeto a la dignidad de la persona"[63]; destacamos que el uso de las Tics en las relaciones comerciales supone también el tratamiento de información de carácter personal. Así, en la sociedad de la información, la protección de bienes jurídicos relacionados con la privacidad y los datos personales adquieren especial importancia, a partir de la implantación de procesos relacionados con la firma electrónica y documentos electrónicos. Por ello, subrayamos que "las nuevas tecnologías son una oportunidad histórica para fortalecer la Administración y para mejorar el respeto al derecho

[62] La Ley de Comercio Electrónico, Firmas y Mensajes de Datos se aprobó, mediante la Ley Nro.67 y fue publicada en el Registro Oficial 557 el 17 de abril de 2002.
[63] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 595.

fundamental a la protección de datos personales en la Administración"[64]. Naturalmente, no nos referimos, solo, a la importancia de garantizar el derecho a la protección de datos en el ámbito de la Administración Electrónica sino también a la necesidad de generar la confianza y la seguridad jurídica en el tratamiento de la información que resulte del comercio electrónico[65].

En relación a los principios del tratamiento de la información personal, por vía electrónica o telemática, inicialmente, el art. 9 de la Ley de Comercio Electrónico señalaba que:

> Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta Ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

Por una parte, esta norma introdujo dos novedades. Primero, se hizo referencia al principio del "consentimiento" expreso para asegurar la licitud en el tratamiento de la información, salvo el caso de los datos personales que: a) consten en fuentes accesibles al público; b) se recojan, a partir de funciones propias de la administración; y c) refieran a vínculos contractuales. Y segundo, se reconoce que la protección de datos personales responde al ejercicio de los derechos de

---

[64] Ibíd., 601.

[65] Al respecto, el RGPD determina que "estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas" –Considerando 7–. En este mismo sentido, la Guía Legislativa de la OEA precisa la necesidad de que "la normativa nacional debe proteger el derecho de las personas a beneficiarse de la economía digital y los flujos de información que la sustentan. Debe buscar un equilibrio entre el derecho de las personas a controlar la forma en que se recopilan, almacenan y utilizan sus datos personales y su derecho a tener acceso a los datos, así como los intereses de las organizaciones en el uso de datos personales con fines comerciales legítimos y razonables en una economía basada en datos".

privacidad, intimidad y confidencialidad. Y por otra, advertimos que el texto de dicha norma era similar al art. 6 de la LOPD 15/1999 española, la cual fue derogada por la LOPDGDD 3/2018[66]. Además, precisamos que a diferencia de la Ley de Comercio Electrónico, el RGPD no contiene el concepto de fuentes accesibles al público, sino de satisfacción del interés legítimo[67]. En todo caso, debido a la entrada en vigencia de la LOPD de Ecuador, el art. 9 de dicha Ley ha quedado derogado[68].

Habiendo destacado la relevancia de los principios de privacidad, intimidad y deber de confidencialidad, corresponde añadir que la recopilación, el uso y la cesión o transmisión de los datos personales debe comprometer el consentimiento expreso del titular de los datos personales. Como señala la Guía Legislativa de la OEA, para que el consentimiento tenga validez "la persona debe contar con suficiente información sobre los detalles concretos de los datos que se recopilarán, la forma en que se recopilarán, los fines del procesamiento y toda divulgación que pueda

[66] La LOPD 15/1999, sobre el consentimiento del afectado refería que: "1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la Ley disponga otra cosa; 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado. 3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos; y 4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una Ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado" –art. 6–.

[67] El RGPD señala que el tratamiento será lícito cuando "es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño" –art. 6.1. f)–. En este contexto, "hay que tener en cuenta que la actividad de ponderación que el art. 6.1.f) RGPD –y anteriormente el art. 7.f) de la Directiva 95/46/CE– asigna al responsable del tratamiento implica la realización por parte de éste de un juicio de proporcionalidad, algo más propio de los órganos jurisdiccionales, que supera el principio de responsabilidad proactiva –*accountability*– que el RGPD atribuye al responsable –art. 2.2 y 24–.". Cfr. Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 225.

[68] Cfr. Disposición derogatoria primera de la LOPD de Ecuador de 2021.

efectuarse". En todo caso, exigiéndose que el consentimiento sea expreso, un elemento positivo es que "posiblemente, la mejora de las tecnologías de la comunicación ha facilitado la posibilidad de exigir el consentimiento explícito, algo que en el pasado podía ralentizar la relación jurídica en Internet"[69]. Con referencia a este aspecto, conviene señalar que para el año de promulgación de la Ley de Comercio Electrónico no se consideraba a la protección de datos como un derecho fundamental, por lo que el consentimiento expreso significó, en realidad, un gran avance en el marco de protección de la información personal[70].

Ahora bien, el art. 21 del Reglamento de la Ley de Comercio Electrónico hace referencia a la seguridad en la prestación de servicios electrónicos[71], señalando que:

> La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la información e instruir claramente sobre los posibles riesgos en que puede incurrir por la falta de dichas seguridades.

Esta norma concreta dos importantes principios dentro del tratamiento de la información. El primer principio se relaciona con la seguridad de datos que, como

---

[69] Antonio Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, Nro. 43 (2012): 25-184.

[70] Como hemos advertido en otro momento, en la Constitución de 1998, vigente en la fecha de promulgación de esta Ley, la protección de datos personales se ejercía, a través de los derechos de privacidad, intimidad y confidencialidad. En este contexto, destacamos que la Novena Disposición General de dicha Ley define tres conceptos que en materia de protección de datos son importantes considerar. Por ejemplo la intimidad, datos personales y datos personales autorizados: "*Intimidad*: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados; *Datos personales*: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley; *Datos personales autorizados*: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular".

[71] El Reglamento de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos se aprobó, mediante el Decreto Ejecutivo Nro.3496 y fue publicado en el Registro Oficial 557 el 31 de diciembre de 2002.

se indicó, anteriormente, está incardinado al deber de responsabilidad de los encargados del tratamiento[72]; y el segundo principio es el deber de información[73]. Si bien existe una referencia, tanto al deber de información sobre el fundamento jurídico del tratamiento como a la forma de almacenamiento y la dirección e identidad del encargado de manejarlos; apuntamos que el derecho a la información, en materia de protección de datos, tiene características mucho más amplias. Como indicamos, este derecho "atribuye a la persona un conocimiento y, por tanto, facilita un control sobre sus datos personales sometidos a tratamiento, de manera que pueda, en su caso, prestar el consentimiento y ejercitar sus derechos"[74].

Además, el art. 21 del Reglamento introduce el concepto jurídico de datos sensibles del consumidor, regulando el ejercicio de las facultades de control sobre dichos datos. Así, se determina que:

> Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten. Por el incumplimiento de las disposiciones contenidas en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones.

En este mismo ámbito, el art. 21.2 del Reglamento también hace referencia a los datos sensibles del consumidor y que tienen que ver con informaciones que pueden derivar en fraudes o ilícitos, que afecten al titular de la información. Sobre este respecto, advertimos que:

> La voluntad de mejorar la protección de los datos personales en el ámbito de las tecnologías de la información y las comunicaciones aconseja alcanzar algunas sinergias con la industria

[72] Como señala la Guía Legislativa de la OEA, "la obligación específica consiste en proporcionar salvaguardias razonables y adecuadas. Se basa en la consecución y el mantenimiento de un nivel apropiado de atención en el contexto de la situación general. Por lo tanto, hay que tener en cuenta consideraciones de proporcionalidad y necesidad".

[73] Asimismo, la Guía Legislativa de la OEA expresa la necesidad de que se informe a los titulares de los datos personales "sobre el fundamento jurídico de la recopilación de sus datos personales, la forma en que se almacenarán y procesarán, la identidad de los encargados de manejar esos datos e información para contactarlos".

[74] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 453**.**

> de las TIC, para tratar de que los equipos informáticos y el software estén fabricados de una manera que permita el control de los propios datos personales[75].

Es importante considerar las referencias del Reglamento al ejercicio del derecho a la rectificación de información falsa o inexacta, como una facultad de control y de garantía de dominio de la información personal –art. 21.3–. Como hemos señalado en otro momento, la protección de datos y el *habeas data* constituyen un derecho fundamental en sí mismo, cuya finalidad en sede jurisdiccional se orienta a garantizar "la facultad de comprobar si la información es actualizada y correcta y, de no serlo, solicitar y obtener su actualización o rectificación"[76].

Sobre estas importantes novedades, la Corte Nacional de Justicia consideraba que debía aplicarse la regla contenida en el art. 9.2 –actualmente, derogado– de la Ley de Comercio Electrónico, en lo relacionado al consentimiento[77]. Por tanto, la Segunda Sala de lo Laboral y Social expuso que:

> Sobre el hecho de que se ha ignorado por parte de los juzgadores la protocolización del acta notarial de diligencia de constatación de 24 de agosto de 2004; ello tiene su razón de ser en que ésta no puede constituir prueba válida, pues el que se haya protocolizado por un Notario (fjs. 14 a 28) no la convierte en prueba válida, ya que en la especie, el Notario Cuadragésimo del Cantón Quito (…) se aparta de las normas constitucionales y las legales aplicables (…) al respecto debe recordarse que por expreso mandato constitucional, las pruebas obtenidas o actuadas con violación de la Constitución o la Ley, no tendrán validez alguna (Art. 24 numeral 14); y el Art. 9 inciso segundo de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos (RO.S. Nro. 557 de 17 de abril de 2002), determina: "La recopilación y (uso de datos personales) responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta Ley, (los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente).": (el subrayado es nuestro ( )), circunstancias que en la especie no se encuentran, puesto que el señor González, no autorizó se utilicen sus datos personales (correos electrónicos), ni existió orden de autoridad competente que lo permita, por ende el Notario no podía realizar tal diligencia; por tanto, el informe emitido por el perito designado no se constituye en prueba, pues éste deviene de la protocolización realizada por el Notario.

Tomando en consideración el año de promulgación, tanto de la Ley de Comercio Electrónico como de su Reglamento, son pocos los criterios judiciales que se han desarrollado en la materia con el objeto de afianzar la regulación del tratamiento de la información personal. Quizá, una de las principales causas sea el grado de

---

[75] Ibíd., 604**.**

[76] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 119.

[77] Véase la sentencia contenida en la Gaceta Judicial. Año CVII. Serie XVIII, Nro. 2. Página 655, del 15 de noviembre de 2004.

desconocimiento de la terminología que se encuentra vinculada a la protección de datos en la sociedad de la información. En todo caso, consideramos que la LOPD –que de manera integral recoge los principios, derechos y obligaciones– supondrá que su garantía en los servicios de la administración electrónica no pase desapercibida.

## 2.4 La protección de datos personales en la Administración de Justicia

### A. Código de la Niñez y la Adolescencia

Como hemos destacado, la protección de datos personales de la niñez y la adolescencia tiene especial trascendencia, por cuanto "en el seno de una sociedad tecnológicamente avanzada cada sujeto va forjando, desde su nacimiento, a través de su infancia y de su madurez hasta su muerte, un amplio y, en ocasiones, complejo y prolijo, catálogo de informaciones"[78]. Sobre la base del principio de interés superior, es imprescindible garantizar que, en los procesos de administración de justicia, el tratamiento de la información respete los derechos y libertades fundamentales de los menores.

En relación al derecho a la reserva de la información de los antecedentes penales, el art. 54 del CNA determina que:

> Los adolescentes que hayan sido investigados, sometidos a proceso, privados de su libertad o a quienes se haya aplicado una medida socio - educativa, con motivo de una infracción penal, tienen derecho a que no se hagan públicos sus antecedentes policiales o judiciales y a que se respete la reserva de la información procesal en la forma dispuesta en esta Ley, a menos que el Juez competente lo autorice en resolución motivada, en la que se expongan con claridad y precisión las circunstancias que justifican hacer pública la información.

El deber de secreto, reserva o confidencialidad de la información es un presupuesto esencial del derecho a la protección de datos. Por tanto, en esta parte haremos referencia a la excepcionalidad de hacer pública la información personal, particularmente, en el sistema de administración de justicia. Así, por ejemplo, la Guía Legislativa de la OEA sugiere que los datos personales que obran en poder

[78] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 188.

de organismos gubernamentales –como en este caso, las autoridades judiciales–, podrían hacerse públicos y no vulneraría el principio de confidencialidad, siempre y cuando se autoricen "por medio de disposiciones claras y específicas".

Si bien el CNA, como parte del principio de transparencia, faculta a que la autoridad competente autorice la publicación de información personal, se requiere que dicha autorización se haga, mediante una resolución motivada con exposición de fundamentos claros y precisos[79]. Esta previsión es sustancial, toda vez que la divulgación excesiva de información personal puede derivar en restricciones ilegítimas sobre el ejercicio de las libertades del titular de los datos. Sobre este aspecto, es necesario señalar que la LOPD –sobre el derecho de los menores a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas– ha establecido una prohibición expresa, en lo que respecta al tratamiento de datos de la niñez y la adolescencia, a menos que "se cuente con la autorización expresa de su representante legal; o, cuando dicho tratamiento esté destinado a salvaguardar un interés público esencial" –art. 21–.

De este modo, insistimos en que, "el mal uso de los datos personales puede traer como consecuencia la restricción ilegítima de derechos tales como el de libertad de circulación, libertad religiosa, libertad de sindicación, acceso a funciones públicas, o el derecho al trabajo"[80]. Así, en lo que corresponde a la niñez y a la adolescencia, el tratamiento ilegítimo de su información puede derivar, en el futuro, en intromisiones, que afecten a sus derechos de igualdad y no discriminación. Además, recordemos que cualquier información y comunicación, cuyo tratamiento les perjudique debe hacerse en un lenguaje claro y sencillo. Así, lo entiende la LOPD cuanto dispone que, en el caso de los adolescentes, "a partir de los 15 años, podrán otorgar, en calidad de titulares, su consentimiento explícito para el tratamiento de

[79] Recordemos que el RGPD determina que el principio de transparencia "exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice" –Considerando 58–.
[80] Pablo Lucas Murillo de la Cueva y José Luis Piñar, El *derecho a la autodeterminación informativa* (Madrid-México: Fontamara S.A, 2011), 109.

sus datos personales, siempre que se les especifique con claridad sus fines" –art. 21–.

Por otra parte, en los procesos de administración de justicia en que intervienen menores, la práctica de las pruebas también conlleva el tratamiento de información personal[81]. Según dispone el CNA para la práctica de exámenes médico legales de los niños, niñas y adolescentes "se practicarán en estrictas condiciones de confidencialidad y respeto a la intimidad e integridad física y emocional del paciente" –art. 80–. Al respecto, puntualizamos que:

> La decisión sobre el acceso a la información médica debe ser adoptada por el facultativo responsable de la asistencia del menor, que deberá valorar, por un lado, la conveniencia de comunicar a los padres la enfermedad o tratamiento, para que ellos, titulares de la patria potestad, puedan ejercitar correctamente sus deberes y velar por la salud de sus hijos[82].

Con el objeto de evitar intromisiones ilegítimas en la información médico legal de la niñez y la adolescencia, observamos que el CNA reconoce como una "garantía de reserva" a la protección de la intimidad, considerando que "se respetará la vida privada e intimidad del adolescente en todas las instancias del proceso" –art. 317–. Además, se han previsto sanciones para los casos que amenacen o vulneren este derecho. Por ejemplo, quien infrinja derechos –relacionados a la intimidad y a la imagen– de los niños, niñas y adolescentes será condenado por cada amenaza o violación de éstos al pago de una multa de 100 a 500 USD[83]. En todo caso, como

[81] La Ley Orgánica de la Función Judicial que estuvo vigente hasta inicios de 2009 establecía que: "Los trámites judiciales son esencialmente públicos, con las excepciones que la Ley establece. Se prohíbe a los jueces dar trámite a informaciones sumarias o diligencias previas que atenten a la honra y dignidad de las personas o a su intimidad" –art. 201–. En la actualidad, sobre el principio de publicidad de los procesos judiciales, el Código Orgánico de la Función judicial determina que: "Las actuaciones o diligencias judiciales serán públicas, salvo los casos en que la Ley prescriba que sean reservadas. De acuerdo a las circunstancias de cada causa, los miembros de los tribunales colegiados podrán decidir que las deliberaciones para la adopción de resoluciones se lleven a cabo privadamente. No podrán realizase grabaciones en video de las actuaciones judiciales. Se prohíbe a las juezas y a los jueces dar trámite a informaciones sumarias o diligencias previas que atenten a la honra y dignidad de las personas o a su intimidad" –art. 13–.

[82] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 174.

[83] Sobre este aspecto, la Guía Legislativa de la OEA señala que "en los casos en que se imponen sanciones a los controladores de datos por incumplimiento del deber de salvaguardar y proteger, tales sanciones deberían ser proporcionales al grado de perjuicio o de riesgo. En este contexto podría ser útil que las jurisdicciones nacionales adoptaran definiciones específicas de lo que constituye una "violación" (o "acceso no autorizado"), los tipos de datos que podrían requerir un grado

se verá más adelante, dentro de nuestro ordenamiento jurídico, existen normas específicas que se destinan a sancionar, desde el ámbito penal el incumplimiento de las garantías previstas para la protección de la información personal.

Hay que destacar que el Consejo de la Judicatura de Ecuador cuenta con un Estatuto de Gestión Organizacional que regula el acceso a la información personal, que obra en los expedientes judiciales[84]. Dicha norma dispone que dentro de la gestión administrativa de este organismo se debe "mantener estricta reserva de la correspondencia y documentos que ingresen", y así también "supervisar la correcta aplicación de las políticas, normas y procedimientos establecidos por la Secretaría General, para la adecuada administración de documentos y archivos a nivel provincial". Entre las políticas, normas y procedimientos para la adecuada administración de los documentos, especial importancia comportan aquellas que se relacionan con las salvaguardias tecnológicas. Así, el referido Estatuto garantiza "preservar la confidencialidad, integridad y seguridad de la infraestructura tecnológica y de la información que se procesa, almacena o transmite a través de los diferentes sistemas informáticos institucionales".

Dentro de la gestión de los procesos que se tramitan en el Consejo de la Judicatura, la Subdirección Nacional de Archivo y Gestión Documental se encarga de "elaborar proyectos de instructivos, manuales, normas técnicas archivísticas y de gestión documental, para los archivos jurisdiccionales, administrativos y notariales". Esta instancia cuenta con un "Protocolo genérico de manejo documental y archivístico para las Unidades Judiciales" que, en relación al tratamiento de la información de carácter personal, señala:

> No se entregarán las causas, sin autorización expresa del titular, que contengan información de circulación restringida o temas de carácter reservado que establece la Ley como, por ejemplo: violencia intrafamiliar, casos penales en los que se encuentre vinculado un menor, violación, menores infractores, causas en las cuales se posea información que pueda atentar contra la seguridad nacional, aquella que esté protegida expresamente con una cláusula de reserva previamente establecida en la Ley. La información acerca de datos de carácter

mayor de protección en esos casos y las responsabilidades específicas que podría tener un controlador de datos en caso de una divulgación de ese tipo".

[84] El Estatuto de Gestión Organizacional del Consejo de la Judicatura (que incluye la cadena de valor; su descripción y mapa de procesos) fue aprobado, mediante Resolución del Consejo de la Judicatura Nro. 70 y, publicado en el Registro Oficial Edición Especial Nro. 158 el 30 de julio de 2014.

> personal y la que provenga de las comunicaciones personales cuya difusión no haya sido autorizada expresamente por su titular, por la Ley o por la o el juzgador. La información producida por la o el fiscal en el marco de una investigación previa y aquella originada en la orden judicial relacionada con las técnicas especiales de investigación. La información acerca de niñas, niños y adolescentes que viole sus derechos según lo establecido en el Código Orgánico de la Niñez y Adolescencia y la Constitución. La información calificada por los organismos que conforman el Sistema nacional de inteligencia y la demás contenida en la legislación pertinente[85].

En este orden, frente a la confidencialidad y la intimidad en los procesos judiciales que involucren a niños, niñas y adolescentes, el Expediente de Casación 896 – Caso signado con el Nro. 896-2009– de la Segunda Sala de lo Penal de la Corte Nacional de Justicia señala que:

> En cuanto al argumento del recurrente en el sentido de que, al haberse practicado la diligencia de reconocimiento médico legal únicamente con la comparecencia del Perito, la ofendida y su madre, se ha violentado lo preceptuado en el Art. 11 y 116 del Código de Procedimiento Penal, ya que no se le permitió al procesado o su abogado estar presente en esta diligencia. Al respecto es importante dejar en claro que en los delitos de carácter sexual y de aborto los peritos practicarán el reconocimiento sin la presencia del fiscal y del secretario, así lo establece el Art. 103 del Código de Procedimiento Penal, más aún el Art. 80 del Código de la Niñez y Adolescencia, señala expresamente que "Los exámenes médicos legales a un niño, niña o adolescente se practicarán en estrictas condiciones de confidencialidad y respeto a la intimidad e integridad física y emocional del paciente".

Tanto el CNA, como las resoluciones del Consejo de la Judicatura, han desarrollado normativa que garantiza en el sistema judicial la protección de la información personal de los niños, niñas y adolescentes. La tutela de los datos personales, en el contexto de la administración de justicia, se sustenta en la garantía de los derechos y bienes jurídicos relacionados con la intimidad, confidencialidad y deber de responsabilidad, a partir de las injerencias arbitrarias en la vida privada. Tomando en cuenta que la Guía Legislativa de la OEA aconseja que “el reto consiste en proporcionar orientación válida a los controladores de datos, procurando al mismo tiempo que las normas sigan siendo “tecnológicamente neutrales” y que no se vuelvan obsoletas como consecuencia de los rápidos cambios tecnológicos”. Los esfuerzos desarrollados, institucionalmente, por el Consejo de la Judicatura, para precautelar el derecho a la protección de datos en el sistema de administración de justicia, no deben pasar inadvertidos. Naturalmente, es necesario que dichas disposiciones se ajusten a la actual LOPD, en cuanto a respetar “los criterios de

[85] El Protocolo genérico de manejo documental y archivístico para las Unidades Judiciales fue elaborado el 1 de mayo de 2014 (Código: SG-SNAGD-01).

legalidad, proporcionalidad y necesidad, y además incluir salvaguardas específicas para proteger los derechos fundamentales de los interesados" –art. 21–. En todo caso, además, nos parece necesario que a este esfuerzo deben sumarse campañas que enfaticen en los servidores judiciales el deber de guardar el secreto y la confidencialidad de la información personal, que obra en los expedientes judiciales.

### B. Código Orgánico Integral Penal

En el Derecho Penal es muy común la normativa destinada a garantizar el derecho a la intimidad y a la protección de datos personales. Como hemos destacado, este derecho se configura como un instituto de garantía de otras libertades. Considerando que uno de esos derechos es la intimidad, el art. 5.10 del Código Orgánico Integral Penal señala que el debido proceso penal se regirá, entre otros principios, por la protección de la intimidad personal y familiar. Además, garantiza el derecho a la privacidad y a la confidencialidad de las víctimas de delitos sexuales y de los menores que participen en un proceso penal –art. 5.20–[86].

En cuanto a los tipos penales, sobre delitos contra el derecho a la intimidad personal y familiar –en lo que cabe a la difusión o publicación de datos personales–, dicha norma sanciona en el art. 178 la violación a la intimidad, considerando que:

> La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

Sobre los delitos contra la seguridad de los activos de los sistemas de información y comunicación, el art. 229 del Código Orgánico Integral Penal sanciona la revelación ilegal de bases de datos, mediante la violación del secreto, intimidad y privacidad de las personas, tipificando que:

[86] El Código Orgánico Integral Penal se aprobó, mediante la Ley Nro.0 y fue publicada en el Registro Oficial Nro. 180 el 10 de febrero de 2014. Por ejemplo, en materia de protección de datos personales, el art. 5.20 prohíbe: "divulgar fotografías o cualquier otro dato que posibilite su identificación en actuaciones judiciales, policiales o administrativas y referirse a documentación, nombres, sobrenombres, filiación, parentesco, residencia o antecedentes penales".

> La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Por otra parte, en las audiencias penales, se impone a todas las personas que intervienen en el proceso el "deber de guardar reserva sobre lo que ven, oyen o perciben; y reserva de identidad sobre datos personales de los sujetos procesales, terceros o de otros participantes en el proceso" –art. 566–.

En este ámbito de regulación, la Guía Legislativa de la OEA advierte que "la incidencia creciente de intrusiones externas ("violaciones de los datos personales"), que consisten en el acceso no autorizado a datos protegidos, suscita preocupaciones relacionadas con la privacidad y con el ámbito penal". Por ello, es imprescindible que, en el sistema de administración de justicia penal, el tratamiento de datos personales cumpla con los principios esenciales, que exige el derecho a la protección de datos. Hablamos en esta parte de los principios de confidencialidad y consentimiento, por cuanto si bien el Código Orgánico Integral Penal, consagra como principio procesal a la publicidad en los procesos penales –art. 5.16–, al mismo tiempo garantiza la privacidad y la confidencialidad –art. 5.20–.

Reiterando que la confidencialidad, el consentimiento y las medidas de seguridad son necesarias a la hora del tratamiento de la información personal en el ámbito penal, catalogamos esta categoría de datos como sensibles o especialmente protegidos. Por esta razón, "la definición de estos datos como especialmente protegidos tiene consecuencias, sobre todo en lo que hace referencia al consentimiento para el tratamiento, así como en la determinación de las medidas de seguridad aplicables"[87]. En todo caso, recordemos que el RGPD regula esta cuestión como un supuesto de legitimación del tratamiento de datos "cuando los tribunales actúen en ejercicio de su función judicial" –art. 9.2. f)–, lo cual, por

[87] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 467,468.

ejemplo, “sería también aplicable a los médicos que piden el acceso a historias clínicas de pacientes a los que ya no dan asistencia para defenderse ante demandas judiciales”[88].

Hemos reiterado que el tratamiento de la información de carácter personal puede derivar en la vulneración de los derechos y libertades fundamentales de los titulares de los datos. Por ejemplo, el ejercicio del derecho de libertad puede considerarse como una de las posibles afectaciones a situaciones vinculadas con el derecho a la intimidad. En este caso, la Resolución 47 –Caso signado con el Nro. 9-12-IN– de la CCE considera que:

> El derecho a la libertad general de acción como libertad negativa, comprende prima fase el derecho de hacer u omitir lo que quiera, en el caso del derecho a la libertad de expresión y de prensa, e incluso el derecho de poder expresar frases ofensivas, discriminatorias, así como a develar públicamente actos íntimos que afecten el honor, la honra y el núcleo esencial que es el buen nombre, hechos que sin duda afectarían los derechos de los demás. Sin embargo, dado que esta libertad no es absoluta y debe armonizarse con la exigencia de otros derechos, por ejemplo, el derecho a la honra y el buen nombre (artículo 66 numeral 18 de la Constitución de la República del Ecuador), puede ser restringida por el legislador, quien legítimamente puede imponer una norma restrictiva de esa libertad de prensa. Los derechos no son absolutos, sino que se relativizan respecto de otros (…) Es claro que estas normas hacen referencia a establecer las áreas hasta donde debe llegar la libertad de información, como es el caso del derecho a la intimidad y la información, que por seguridad del Estado deben ser autorizadas mediante Ley (…) Por tanto, cualquier afectación al derecho a la honra acarrea la debida protección por parte del Estado, a través del derecho penal, el establecimiento de sanciones y penas que ayuden a reparar el derecho vulnerado. (…) Consecuentemente, aquellas personas que reproduzcan artículos o imágenes injuriosos son responsables del delito sin que puedan argumentar en su favor, el nombre de la persona o personas que elaboraron en un inicio, dichos artículos o imágenes. Tampoco pueden excusarse en que se trata de una simple reproducción de una publicación o imagen ya existente. En este sentido, la norma, conforme se evidencia, protege el derecho al honor y al buen nombre, en la medida que castiga a aquella persona que reproduce una injuria. En consecuencia, esta Corte no advierte la manera en que este artículo es inconstitucional.

Es fundamental que, desde el ámbito penal, se regule la tutela y sanción de las acciones u omisiones que afecten el derecho a la protección de datos, toda vez que “estas garantías, comunes al funcionamiento de cualquier banco de datos, asumen especial trascendencia en el sector judicial, por la relevancia política, económica, social y cultural que reviste la documentación en los procedimientos judiciales”[89].

---

[88] Troncoso, “Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales”, 234.

[89] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 56.

Naturalmente, habrá que considerar la necesidad de respetar, en el ámbito judicial, las excepciones para el tratamiento de categorías especiales de datos personales, bien, mediante la LOPD o, a través de las reformas necesarias, tanto al Código Orgánico Integral Penal como a la normativa que regula el tratamiento de la información en el Consejo de la Judicatura. En todo caso, en este ámbito, un buen ejemplo representa la Ley Orgánica 7/2021 de España, por la cual se regula la protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales[90].

### C. Código Orgánico General de Procesos

El Código Orgánico General de Procesos está llamado a resolver dentro del sistema procesal –excepto en materia constitucional y penal– la armonización de los principios aplicables a las actuaciones procesales. Esta Ley tiene por objeto garantizar la tutela judicial efectiva y demás principios constitucionales, dentro del sistema procesal ecuatoriano[91]. Así, en relación a la protección de los datos personales de las partes procesales, el art. 7 de este Código refiere que:

> Las y los juzgadores garantizarán que los datos personales de las partes procesales se destinen únicamente a la sustanciación del proceso y se registren o divulguen con el consentimiento libre, previo y expreso de su titular, salvo que el ordenamiento jurídico les imponga la obligación de incorporar dicha información con el objeto de cumplir una norma constitucionalmente legítima.

Además, en relación al principio de transparencia y publicidad de los procesos judiciales, establece que "únicamente se admitirá aquellas excepciones

[90] La Ley Orgánica 7/2021 representa una novedad, en el ámbito internacional, puesto que, su finalidad principal es que "los datos sean tratados por estas autoridades competentes de manera que se cumplan los fines prevenidos a la par que establecer los mayores estándares de protección de los derechos fundamentales y las libertades de los ciudadanos, de forma que se cumpla lo dispuesto en el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, así como en el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea y el artículo 18.4 de la Constitución". Cfr. https://www.boe.es/buscar/act.php?id=BOE-A-2021-8806.
[91] El Código General de Procesos se aprobó, mediante la Ley Nro.0 y fue publicada en el Registro Oficial 506 el 22 de mayo de 2015.

estrictamente necesarias para proteger la intimidad, el honor, el buen nombre o la seguridad de cualquier persona" –art. 8–. Al igual que las disposiciones del Código Orgánico Integral Penal, indicamos que la información procesal es pública. No obstante, el Código Orgánico General de Procesos también reconoce que la información puede ser restringida, en virtud de proteger la intimidad, el honor, el buen nombre o la seguridad de cualquier persona.

En el tratamiento de datos personales se exige el respeto y garantía del principio de pertinencia, bajo el cual la información personal, únicamente, debe ser tratada, según los fines para los cuales fue recaba. Por tanto, el consentimiento del titular de los datos personales puede legitimar que dichos datos sean divulgados. Esto es, particularmente, esencial, por cuanto dentro del marco de protección de datos, el consentimiento constituye un principio que puede aplicarse, no solamente al tratamiento sino también cuando se trata de cesiones de datos o divulgaciones a terceros. No obstante, en el presente caso deberá considerarse la necesidad de plantear excepciones como un supuesto de legitimación, frente al tratamiento de la información personal, cuando las autoridades judiciales actúen en el ejercicio de sus funciones.

Es importante destacar que, por primera ocasión dentro del sistema de gestión de procesos en la Administración de Justicia, esta Ley incorporó la figura del "expediente electrónico". Tomando en cuenta que "la administración electrónica y la integración de las tecnologías de la información en los servicios públicos es un factor fundamental para el desarrollo de la sociedad de la información"[92]; resaltamos que los procesos de gestión administrativa han evolucionado de procesos manuales a procesos tecnológicos. Así, la llamada administración electrónica supone que el tratamiento de la información, dentro del expediente judicial se ejecute por medios automatizados. En este caso, habrá que tomar en consideración que el RGPD dispone que cuando el tratamiento de datos se haga, a través del uso de nuevas tecnologías y, "entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una

[92] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 574.

evaluación del impacto de las operaciones de tratamiento en la protección de datos personales" –art. 35.1–.

En el caso de la administración de justicia, en nuestro país se trata de un fenómeno, relativamente, nuevo que requiere especial observancia. En la administración, los riesgos se originan, a partir del desconocimiento de los principios que componen el derecho a la protección de datos. Por ello, insistimos en que:

> La informatización documental judicial tiene determinados riesgos, que conviene prevenir. Deberá garantizarse, en primer término, la calidad de los datos jurídicos almacenados, lo que equivale a proteger la veracidad y objetividad de la información seleccionada, así como la mayor exhaustividad posible de la misma y su continua actualización. Se precisan también medidas cautelares que velen por la seguridad de los datos almacenados (*storage*) para evitar la destrucción accidental, o la cancelación no autorizada, la pérdida, o la manipulación de las informaciones jurídicas[93].

Desde esta perspectiva, en relación a la naturaleza del expediente electrónico, el art. 115 de este Código determina que:

> Es el medio informático en el cual se registran las actuaciones judiciales. En el expediente electrónico se deben almacenar las peticiones y documentos que las partes pretendan utilizar en el proceso. Las reproducciones digitalizadas o escaneadas de documentos públicos o privados que se agreguen al expediente electrónico tienen la misma fuerza probatoria del original. Los expedientes electrónicos deben estar protegidos por medio de sistemas de seguridad de acceso y almacenados en un medio que garantice la preservación e integridad de los datos.

Así, la seguridad de datos se presenta como un principio que garantiza que el tratamiento de la información personal se cumpla, por medio de condiciones de seguridad razonables y adecuadas, ya que significa "una garantía de la integridad, de la disponibilidad y de la confidencialidad de la información"[94]. Por ello, a través de este principio es conveniente que en el expediente electrónico se garantice la preservación e integridad de la información. En todo caso, "si bien la actividad de la Administración Pública debe orientarse al principio de eficacia, dicho principio no debe ser interpretado de forma independiente, sino en consonancia con todo el ordenamiento jurídico y con los derechos fundamentales"[95]. Desde esta perspectiva, pese a la normativa del Consejo de la Judicatura, reiteramos la necesidad de

[93] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 55,56.
[94] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 474,475**.**
[95] Ibíd., 595.

establecer sistemas de seguridad electrónica para los expedientes, con el objeto de garantizar su preservación e integridad, lo cual supone, irremediablemente, precisar sus efectos, frente a la protección de la información de carácter personal.

Al respecto, apuntamos que:

> Aún más: solo si protegemos los datos personales podemos establecer la relación de confianza necesaria para el desarrollo de las nuevas tecnologías de la información y la comunicación en la sociedad y en las Administraciones Públicas. Por tanto, para que la Administración electrónica se implante y se desarrolle, es necesario respetar la legislación de protección de datos personales[96].

La protección de datos personales en la administración electrónica es un reto que, todavía, está pendiente. Sobre todo, en cuanto a garantizar el principio de seguridad de la información personal, ya que, únicamente, se ha desarrollado en un Estatuto y Protocolo que pertenece al Consejo de la Judicatura. Hacen falta previsiones que deben enmarcarse en la LOPD y puedan ser aplicadas en el sistema de administración de justicia, por cuanto la nueva normativa de protección de datos plantea que "los datos personales cuyo tratamiento se encuentre regulado en normativa especializada estarán sujetos a los principios establecidos en sus propias normas y los principios establecidos en esta Ley" –art. 11–. Como se ha analizado, el tratamiento de información personal vinculado a procesos tecnológicos conlleva también la obligación que, desde el Estado se ejecuten las medidas de vigilancia y aplicación de principios relativos al derecho fundamental a la protección de datos personales.

## 2.5 La protección de datos personales en el Régimen Tributario

### A. Ley Orgánica de Régimen Tributario

En el ejercicio de la administración tributaria, la actividad controladora del pago de impuestos comporta también un tratamiento de datos. Las atribuciones que puedan asignarse a la administración, en muchos casos, podrían considerarse como intromisiones en las facultades que se desprenden del derecho a la protección de

[96] Ibíd., 600-601.

datos. En primer término, apuntamos que el RGPD plantea que el tratamiento de datos es lícito cuando se haga “para el cumplimiento de una obligación legal aplicable al responsable del tratamiento” –art. 6.1. c)–; y también “para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento” –art. 6.1. e)–. Por otra parte, como una excepción en los datos personales especialmente protegidos, el RGPD permite el tratamiento por razones de interés público “que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado” –art. 9.2. g)–; y que, en todo caso, se extiende al ámbito fiscal, cuando el RGPD permite limitar el alcance de ciertos derechos y obligaciones relacionados a la protección de datos –art. 23.1. e)–.

Como queda anotado, el RGPD plantea algunas excepciones, limitaciones y condiciones de licitud en el tratamiento de la información, que afectan el ejercicio de las Administraciones Públicas Tributarias. Ahora bien, hay que considerar qué sucede con la información que pueda requerirse a la Administración Tributaria y que contenga datos personales. Frente a este supuesto, por ejemplo, la LOPDGDD reconoce, dentro del deber de colaboración en las Administraciones Públicas, que “cuando la información contenga datos personales la comunicación de dichos datos estará amparada por lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679” –art. 52.1–. Es decir, el tratamiento será lícito, por cuanto procede de la observancia de una obligación legal.

La Ley Orgánica de Régimen Tributario regula algunos escenarios vinculados con el tratamiento de la información personal de los contribuyentes[97]. Por ejemplo, sobre las operaciones de los contribuyentes, esta Ley señala que “la información presentada por los contribuyentes, conforme este artículo, tiene el carácter de reservada” –art. 22–. Así también, en relación a la información contenida en las declaraciones e informaciones de los contribuyentes, el art. 101 precisa que:

[97] La Ley Orgánica de Régimen Tributario se aprobó mediante Codificación N0. 26 y fue publicada en el Registro Oficial Suplemento 463 el 17 de noviembre de 2004.

> Las declaraciones e informaciones de los contribuyentes, responsables o terceros, relacionadas con las obligaciones tributarias, así como los planes y programas de control que efectúe la Administración Tributaria son de carácter reservado y serán utilizadas para los fines propios de la administración tributaria. La información que contribuya a identificar la propiedad y las operaciones de los residentes en el Ecuador con terceros ubicados en paraísos fiscales, así como las prácticas de planificación fiscal agresiva, no estarán sujetas a la reserva establecida en este artículo. Tampoco tendrá el carácter de reservado la información relacionada con los asesores, promotores, diseñadores y consultores de estas prácticas.

La administración tributaria debe enmarcar su gestión en el respeto y garantía de los derechos que se derivan de la protección de datos. La excepción a esta regla –y por consiguiente al carácter reservado de la información tributaria de los contribuyentes– tiene como base el interés legítimo de la administración y la justificación, sobre la trascendencia tributaria de obtener información asociada con la posible evasión de impuestos en paraísos fiscales. Vinculada a esta facultad, el art. 106 de esta Ley ha previsto que en el requerimiento de la información por parte de la administración tributaria no existirá reserva ni sigilo que le sea oponible. Así, se determina que:

> Las personas naturales o jurídicas, nacionales o extranjeras domiciliadas en el país, que no entreguen la información requerida por el Servicio de Rentas Internas, dentro del plazo otorgado para el efecto, serán sancionadas con una multa de 1 a 6 remuneraciones básicas unificadas del trabajador en general, la que se regulará teniendo en cuenta los ingresos y el capital del contribuyente, según lo determine el reglamento. Para la información requerida por la Administración Tributaria no habrá reserva ni sigilo que le sea oponible y será entregada directamente, sin que se requiera trámite previo o intermediación, cualquiera que éste sea, ante autoridad alguna.

En estos casos no es necesario el consentimiento del titular de la información, así como también solicitar a la autoridad competente la autorización para levantar la reserva o el sigilo de la información solicitada. Esta habilitación se sustenta en el interés legítimo, que en lo esencial debe respetar el derecho a la protección de datos y garantizar medidas necesarias y adecuadas. Por otra parte, la norma citada refiere algunas obligaciones para los responsables del tratamiento de la información, una vez que ésta ha sido recibida. En lo pertinente señala:

> El mal uso, uso indebido o no autorizado de la información entregada al Servicio de Rentas Internas por parte de sus funcionarios será sancionado de conformidad con la normativa vigente. La información bancaria sometida a sigilo o sujeta a reserva, obtenida por el Servicio de Rentas Internas bajo este procedimiento, tendrá el carácter de reservada de conformidad con lo establecido en el inciso final del artículo 101 de la Ley de Régimen Tributario Interno únicamente y de manera exclusiva podrá ser utilizada en el ejercicio de sus facultades legales. El Servicio de Rentas Internas adoptará las medidas de organización interna

> necesarias para garantizar su reserva y controlar su uso adecuado. El uso indebido de la información será sancionado civil, penal o administrativamente, según sea el caso.

La previsión de contribuir en procesos tributarios transparentes y de recaudación de impuestos, que aseguren la redistribución de la riqueza, se prevén como necesarios para el efectivo cumplimiento de los fines de la administración tributaria. No obstante, en este ámbito es esencial salvaguardar las libertades que se desprenden del derecho a la protección de datos, frente al deber de contribuir al gasto social. En este punto, conviene citar la Resolución 38 –Caso signado con el Nro. 10-13-IN– de la CCE que en relación a la normativa expuesta aclara que:

> De la reforma contemplada en el artículo 106 ibidem, se advierte que en virtud de ella, la sanción a los sujetos pasivos en general, se particulariza respecto de las instituciones financieras sujetas al control de la Superintendencia de Bancos y Seguros y las organizaciones del sector financiero popular y solidario, sujetas al control de la Superintendencia de Economía Popular y Solidaria (…) De otra parte se estipula que para la información requerida por la Administración Tributaria no habrá reserva ni sigilo que le sea oponible, "y será entregada directamente, sin que se requiera trámite previo o intermediación, cualquiera que éste sea, ante autoridad alguna". (…) En este sentido, lo que el legislador pretende a través de la reforma contenida en la normativa que se analiza es proporcionar a la administración tributaria herramientas suficientes para que cuente con mecanismos de determinación, control y recaudación del impuesto a la renta, del IVA y del ISD, lo que a su vez, permiten al contribuyente comprender cuál es el hecho generador del tributo y el modo en que debe cumplir con su obligación (…) Del análisis de la norma que precede, se colige que con dicha reforma se dispuso que todas las entidades del sector público, las sociedades, las organizaciones privadas, las instituciones financieras y las organizaciones del sector financiero popular y solidario; así como las personas naturales estarán obligadas a proporcionar de forma directa al Servicio de Rentas Internas, toda la información que ésta requiera a fin de coadyuvar con el cumplimiento de sus labores de determinación, recaudación y control tributario.

Ahora bien, el ejercicio de la administración tributaria debe traducirse en un control fiscal materializado en solicitudes, debidamente, justificadas con indicación clara del objeto de la solicitud. Tal como señala la CCE, este requisito se prevé, mediante el principio de transparencia del Estado, por el cual:

> La administración tributaria está en la obligación de informar sobre su gestión a la ciudadanía, a fin que los contribuyentes conozcan su operatividad y los procedimientos que deben seguir para cumplir con sus obligaciones tributarias, lo cual guarda conformidad con la norma contenida en el artículo 204 de la Constitución de la República. En efecto, del examen de la normativa acusada, se aprecia que en ella consta el contexto social en que se la aplicará, la especificidad del hecho generador, los sujetos pasivos de la obligación tributaria, así como los beneficios tributarios destinados a incentivar la producción y el desarrollo nacional. (…) De las normas precitadas, se desprende que los cambios realizados están orientados a que los informes requeridos por la administración tributaria no estén sujetos al sigilo bancario, y en concordancia con esta reforma en el literal h) del artículo 91 de la referida norma, se exceptúa de las prohibiciones contempladas para el sigilo y reserva bancaria a cualquier información solicitada por el Servicio de Rentas Internas, de manera

> directa, sin trámite o intermediación alguna, y en las condiciones y forma que esta entidad lo disponga, para sus fines de gestión, control, determinación y recaudación tributaria.

Finalmente, sobre la situación jurídica de esta disposición, frente al derecho a la protección de datos personales, la CCE agrega:

> Del análisis de la citada norma se colige que la misma protege toda información de carácter personal, y prevé que la misma podrá ser revelada, siempre y cuando el titular de ese derecho lo autorice, o si existe una Ley que así lo disponga; es decir, bajo ninguna circunstancia, se obtendrá esta clase de información de forma arbitraria, y para garantizar aquel derecho, la norma en análisis prevé el procedimiento que se debe observar para el efecto. (…) Desde esta perspectiva, se observa que el legislador mediante la norma acusada, no hizo otra cosa que habilitar las facultades, así como los instrumentos jurídicos necesarios y adecuados para que en el marco del debido respeto a los principios y derechos constitucionales, la administración tributaria esté en la posibilidad de hacer su seguridad, estabilidad, transparencia y solidez (…) En este caso, mediante la información obtenida del sector público, privado, y del popular y solidario –que intermedian recursos económicos del público-, al Estado le es posible cumplir con los objetivos de recaudación de impuestos a fin de redistribuir los mismos de forma equitativa en la población. Por consiguiente, la información requerida al contribuyente por el Estado, a través de la administración tributaria, siempre se referirá a aquella proveniente de actividades económicas con relevancia tributaria o fiscal. La información así proporcionada por los contribuyentes a la administración tributaria es de carácter reservado y será utilizada para los fines propios de la administración tributaria, esto es para hacer cumplir funciones, verificar y fiscalizar el cumplimiento de las Leyes tributarias. En virtud de los criterios expuestos, se concluye que a través de la reforma contenida en la normativa que se analiza, únicamente se busca proporcionar a la administración tributaria herramientas suficientes para que a la hora de ejercitar su facultad recaudadora, cuente con mecanismos de determinación, control y recaudación del impuesto a la renta, del IVA y del ISD. En consecuencia, la Corte concluye que la normativa contenida en los artículos 3, 4 y 5 de la Ley Orgánica de Redistribución de los Ingresos para el Gasto Social, no vulnera el derecho a la protección de datos de carácter personal contenido en el artículo 66 numeral 19 del texto constitucional.

Bajo estas consideraciones, el tratamiento de la información en el ejercicio de la administración tributaria se encuentra restringido al respeto del principio de reserva, por cuanto los datos que se obtengan por la Administración Tributaria deben ser utilizados para los fines propios de la administración. Considerando que el tratamiento es lícito cuando se realiza por razones de un interés público, advertimos que el derecho a la intimidad tributaria cede a la hora de poner en práctica las facultades supervisoras de la autoridad de control tributario.

### B. Código Tributario

Asumiendo que la protección de datos personales constituye la capacidad de consentir que la información sea utilizada, adecuadamente, conforme al principio de

finalidad; el tratamiento de la información debe respetar los fines que permiten la recogida de datos. En este aspecto, la Administración Pública al momento de recabar la información personal de los ciudadanos debe garantizar la confidencialidad y la seguridad de ésta. En este contexto, la Administración Tributaria, a través del Código Tributario ha definido la finalidad y la naturaleza de la información tributaria[98]. Este Código prescribe que "las declaraciones e informaciones de los contribuyentes, responsables o terceros, relacionadas con las obligaciones tributarias, serán utilizadas para los fines propios de la administración tributaria" –art. 99–. Así, sobre la norma anotada, la Resolución 781 –Caso signado con el Nro. 781-6-RA– de la CCE expone lo siguiente:

> Siendo así, la autoridad tributaria tiene la facultad de verificar la información proporcionada por el contribuyente y para cruzar información a fin de determinar inconsistencias en la información proporcionada por el contribuyente, pues, la propia Constitución otorga al Estado la facultad de regular y controlar la actividad económica para alcanzar el bien común. Ahora bien, dicha facultad está limitada a solicitar la información relacionada únicamente con las obligaciones que el contribuyente debe satisfacer para con la Administración (…) Tales limitaciones se fundan en que los libros de comercio contienen secretos comerciales que deben ser protegidos (…) Por lo cual, eventualmente, la Administración podría verse precisada, en algún caso concreto, a solicitar u obtener información con orden judicial. OCTAVA.- En el caso concreto, la Administración tributaria ha solicitado la entrega de información (fojas 5 a 7 del expediente de instancia), que si bien es extensa, evidentemente, tiene estricta relación con las obligaciones que el contribuyente debe satisfacer, sin que el contribuyente haya podido demostrar que la información solicitada ya fue entregada a la Administración o que la misma en todo o en parte vulnera el secreto o la privacidad de que gozan, o no tiene relación con las obligaciones tributarias que tiene el contribuyente. Por lo cual, los actos de la administración tributaria no han violado ningún derecho constitucional de la compañía accionante.

Así también, en relación al ejercicio del derecho de acceso a la información personal, que se encuentra legitimado en la acción del *habeas data*; la Resolución 21 –Caso signado con el Nro. 21-2007-HD– de la CCE, en materia de acceso a la información tributaria, determina que:

> La pretensión del accionante es que se le proporcione la información requerida respecto al pago total que la empresa accionada efectuaba por concepto del Impuesto al Valor Agregado IVA, desde el año 2000 hasta el año 2005, ya que éste pago se lo hacía a nombre del compareciente al Servicio de Rentas Internas, así como las facturas de venta señaladas en el ordinal tercero de su líbelo de demanda, es decir, desde el año 2000 hasta el año 2006 ya que el accionado en ningún momento le entregó facturas de venta de los insumos agrícolas así como tampoco de las compras que realizaban de combustible a dicha empresa (…) El accionante tiene derecho a saber cuánto se le retuvo por las transacciones realizadas, inclusive para el momento de declarar sus impuestos. Es indudable que la información que

[98] El Código Tributario se aprobó mediante Codificación Nro.9 y fue publicada en el Registro Oficial Suplemento 38 el 14 de junio de 2005.

> requiere el demandante se refiere única y exclusivamente a su persona, en relación con las transacciones efectuadas con TANASA S.A., y que, en última instancia, tienen que ver con hechos impositivos, razón por la cual es procedente que pueda acceder a la referida información por esta vía que garantiza el derecho de las personas para conocer los datos que sobre ella se encuentre en instituciones públicas o privadas.

De esta manera, en la aplicación de juicios de proporcionalidad entre el derecho a la protección de datos personales y de control tributario del Estado, el derecho a la intimidad, reserva o sigilo de la información cede –por el interés legítimo–, en beneficio del ejercicio de la fiscalización de la autoridad tributaria. En este marco, recordemos que la LOPD dispone que "los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario" –art. 33–. No obstante, para que dicha habilitación respete la normativa de protección de datos, la transferencia de datos debe estar "configurada dentro de una de las causales de legitimidad establecidas en esta Ley, y contar, además, con el consentimiento del titular" –art. 33–. Finalmente, no se observa en este ámbito sectorial disposiciones que regulen las obligaciones de los responsables del tratamiento de información personal, dentro de la administración tributaria. Por tanto, puede considerarse en este sector la necesidad de adoptar códigos de conducta, que facilite la actividad que desarrollen los responsables y encargados del tratamiento[99].

## 2.6 La protección de datos personales en el Régimen Electoral

### A. Código de la Democracia

Otro de los escenarios sobre protección de datos personales, es el que se relaciona con el tratamiento de la información, que proviene de los registros electorales. Este es uno de los regímenes más desprovistos de la normativa que regula la protección

[99] Con referencia a este aspecto, el RGPD establece que los códigos de conducta "podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento" –Considerando 98–.

de este derecho fundamental. La Ley Orgánica Electoral o Código de la Democracia, creada con el objeto de reglamentar los derechos políticos y de participación ciudadana, no reconoce derechos relacionados a la protección de datos personales[100].

Como todo fichero de datos, el padrón o registro electoral debe incorporar principios relacionados con la protección de la información, frente a su tratamiento. Por ejemplo, "–calidad de datos, derecho de información en la recogida de los mismos, seguridad de los datos, comunicación de los datos- y los derechos de las personas en este ámbito –derechos de acceso, rectificación y cancelación–"[101]. Sin embargo, "cuando el acceso a nuestra información personal se produce por quienes nos van a gobernar, al margen de nuestra capacidad de control o conocimiento, saltan las alarmas por la posible manipulación de nuestra voluntad y de nuestra capacidad de decidir"[102]. Por tanto, "una parte de los conflictos que se plantean en materia de protección de datos en unas elecciones —incluida la fase de campaña electoral— conecta, en parte, con el uso indebido que de los datos personales de los electores contenidos en el censo se pueda hacer"[103].

En relación a la información que obra en los registros electorales, el art. 78 del Código de la Democracia refiere que:

> El registro electoral es el listado de personas mayores de dieciséis años, habilitadas para votar en cada elección, es elaborado por el Consejo Nacional Electoral con base en la información que obligatoriamente remitirá el Registro Civil o la entidad encargada de la administración del registro de las personas; se complementará con la inscripción que voluntariamente realicen las y los extranjeros residentes en el país, mayores de dieciséis años para poder ejercer su derecho al sufragio.

En primer término, los padrones o registros electorales no son considerados como información de carácter personal relativa a la ideología, por cuanto sólo contienen

[100] La Ley Orgánica Electoral o Código de la Democracia se aprobó mediante Ley Nro.2 y fue publicada en el Registro Oficial Suplemento 578 el 27 de abril de 2009.
[101] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1014-1015**.**
[102] Mónica Arenas Ramiro, "Partidos políticos, Opiniones políticas e Internet: La lesión del derecho a la Protección de Datos Personales", *UNED: Revista Teoría y Realidad Constitucional,* Nro*.* 44 (2019), 341-372.
[103] Rosario García Mahamut, "Partidos políticos y derecho a la protección de datos en campaña electoral: Tensiones y conflictos en el ordenamiento español", *UNED: Revista Teoría y Realidad Constitucional,* Nro*.* 35 (2015), 309-338.

datos de las personas titulares del derecho al sufragio. Por tanto, solo los padrones de militantes de los partidos políticos constituye información relativa a la ideología política de las personas, y por consiguiente, se trata de datos sensibles o especialmente protegidos[104]. En este sentido, se debe prever una regulación necesaria con el objeto de garantizar que dichos registros cumplan con los principios para el tratamiento de la información de carácter personal, tomando en consideración las suficientes garantías, tanto jurídicas como tecnológicas[105].

La única norma que se relaciona con la protección de datos personales contenida en los registros electorales es el Instructivo para la entrega del Registro Electoral a Organizaciones Políticas, por cuanto determina que las organizaciones políticas y las entidades que soliciten dichos registros se comprometen a "mantener la confidencialidad de la información proporcionada por el Consejo Nacional Electoral. Por ningún motivo o concepto se podrá transferir la información a terceros, en atención a los derechos personales de los sujetos de la información y su alcance" –art. 5–.

Para las organizaciones políticas, la información personal relativa a la ideología política, es fundamental para campañas y mensajes en épocas electorales. Es aquí, donde "se plantea una inédita problemática: la captación y tratamiento ilegítimo de los datos personales de los electores y el uso indebido que de los mismos se puede realizar en un ámbito de marcada confrontación política como son unas

[104] Como expone García Mahamut, ciertamente, "el escenario es complejo y muy preocupante si de lo que hablamos es del acopio y del tratamiento de datos personales con carácter masivo que pueden revelar datos especialmente sensibles como el de ideología política sin el consentimiento expreso de las personas afectadas y sin las adecuadas garantías de confidencialidad y protección". Cfr. García Mahamut, "Partidos políticos y derecho a la protección de datos en campaña electoral: Tensiones y conflictos en el ordenamiento español", 310.

[105] Como apunta Arenas Ramiro, "un claro ejemplo del impacto de esta transformación digital vulnerando la privacidad de los sujetos en un proceso electoral se puso de manifiesto con el conocido caso *Cambridge Analityca*, utilizando información personal de los votantes sin cumplir con las exigencias y garantías previstas en la normativa de protección de datos o en la electoral con el fin de distorsionar el debate político y manipulando la orientación de voto de los votantes gracias a la información que se conocía de los mismos, incluso de manera personalizada gracias a las técnicas de perfilado personalizado basadas en estrategias de marketing (también conocidas como *microtargeting*)". Cfr. Arenas Ramiro, "Partidos políticos, Opiniones políticas e Internet: La lesión del derecho a la Protección de Datos Personales", 343.

elecciones”[106]. Las tecnologías de la información y comunicación han posibilitado que estos procesos se hagan por diversos medios que, en todo caso, “tiene sus beneficios, pero también sus peligros y debemos buscar el equilibrio entre el uso de la información y el respeto por la dignidad y los derechos de los ciudadanos. Esto es esencial para la salud de nuestras democracias”[107]. Así, destacamos que:

> Es habitual que los partidos políticos adapten sus mensajes al público y tengan en cuenta sus intereses específicos con el fin de conseguir el mayor número de votos posible y, por ello, es lógico que estudien cómo utilizar los datos personales de los electores para llegar a ellos de una forma más personalizada, más rentable y con más posibilidad de éxito para sus intereses. Esto ha provocado que los datos personales, la información personal, se conviertan en la nueva moneda de la Revolución digital que vivimos y que los diferentes actores sociales, políticos y económicos quieran tener acceso a los mismos[108]

Con referencia a este aspecto, el Tribunal Constitucional de España ha aclarado que:

> La libertad ideológica comprende «la proclamación de ideas o posiciones políticas propias o adhesión a las ajenas» (STC 235/2007, de 7 de noviembre, FJ 9), tanto individual como colectivamente, así como la posibilidad de abandonarlas o cambiarlas por otras en todo momento, pero también el secreto o silencio sobre las ideas o posiciones políticas propias, sin ser objeto de coacción o perturbación alguna antes o después de su proclamación o modificación, ni derivada del silencio libremente elegido. A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos anteriormente mencionados, también establezca garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental (…) En conclusión, las opiniones políticas son datos personales sensibles cuya necesidad de protección es, en esa medida, superior a la de otros datos personales. Una protección adecuada y específica frente a su tratamiento constituye, en suma, una exigencia constitucional, sin perjuicio de que, como se ha visto, también represente una exigencia derivada del Derecho de la Unión Europea. Por tanto, el legislador está constitucionalmente obligado a adecuar la protección que dispensa a dichos datos personales, en su caso, imponiendo mayores exigencias a fin de que puedan ser objeto de tratamiento y previendo garantías específicas en su tratamiento, además de las que puedan ser comunes o generales[109].

Si bien la información contenida en los padrones de militantes de los partidos políticos tiene particular interés para las organizaciones políticas, subrayamos que

---

[106] García Mahamut, “Partidos políticos y derecho a la protección de datos en campaña electoral: Tensiones y conflictos en el ordenamiento español”, 310.
[107] Arenas Ramiro, “Partidos políticos, Opiniones políticas e Internet: La lesión del derecho a la Protección de Datos Personales”, 344.
[108] Ibíd., 342.
[109] Véase la Sentencia 76/2019, de 22 de mayo de 2019. Recurso de inconstitucionalidad 1405-2019. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2019-9548.

"nada justifica, salvo razones de amenaza democrática, una monitorización permanente, una recopilación o uso permanente de los datos personales de los electores"[110]. Por ello, es "necesario llevar a cabo, en muchos casos, un delicado equilibrio entre el derecho a la autodeterminación informativa y otros derechos fundamentales como el de participación política"[111]. En todo caso, frente a la ausencia de normativa relacionada con la protección del uso de la información personal, por parte de los partidos políticos en este ámbito sectorial, apreciamos que en los sistemas democráticos es esencial establecer, por una parte, garantías adecuadas y, por otra, un justo equilibrio entre el derecho a la protección de datos y los de participación política[112].

### 2.7 Regulación de la información sobre solvencia patrimonial y de crédito

En la actualidad, los derechos de privacidad "afectan a muchos otros aspectos de nuestra vida, entre las que se encuentra nuestra imagen, nuestro trabajo, nuestros hobbies, nuestra familia y relaciones, nuestra situación financiera, e incluso nuestras opiniones, creencias, hábitos de consumo y salud"[113]. Mucha de esta información, indudablemente, permanece en Internet, lo cual implica que puede ser objeto de intromisiones ilegítimas, ocasionando "serios perjuicios tanto morales

[110] Arenas Ramiro, "Partidos políticos, Opiniones políticas e Internet: La lesión del derecho a la Protección de Datos Personales", 362.
[111] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1022.
[112] Tal como prescribe el RGPD, "si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas" –Considerando 56–. En todo caso, a propósito de la Sentencia 76/2019, "el TC señala también que, en este punto, el nivel y la naturaleza de las garantías adecuadas «no se pueden determinar de una vez para todas» y que deben, por un lado, ser revisadas y actualizadas; y, por otro lado, que las mismas deben cumplir con el principio de proporcionalidad, buscando las posibilidades de tratamiento menos intrusivas, lo que variará, por lo tanto, en función del tipo de los datos y de su naturaleza". Cfr. Arenas Ramiro, "Partidos políticos, Opiniones políticas e Internet: La lesión del derecho a la Protección de Datos Personales", 364.
[113] Ignacio Carrasco Salayero, "Cloud Computing", en José López Calvo (coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*. Madrid. Wolters Kluwer. 2018, 250.

(como los datos o imágenes relacionados con la vida íntima o afectiva) o materiales (datos financieros o bancarios)"[114].

Efectivamente, el tratamiento de la información sobre solvencia patrimonial y de crédito puede ocasionar a la persona serios perjuicios materiales, sino se respeta la legislación de protección de datos, a través del derecho al control de los datos. Esto supone, garantizar "la calidad de esos datos objeto de tratamiento, la información y el consentimiento para el tratamiento de los datos, la seguridad de la información y el deber de secreto y el ejercicio de los derechos de acceso, rectificación y cancelación sobre sus datos personales"[115]. En todo caso, como apunta la Guía Legislativa de la OEA, "para los datos más sensibles se requiere un nivel más alto de protección. Algunas de las razones para conferir mayor protección podrían ser, por ejemplo, los riesgos de usurpación de la identidad, pérdidas económicas, efectos negativos en la calificación crediticia".

Según el objeto y finalidad de la Ley del Sistema Nacional de Registros Públicos, se regulan los registros de información crediticia que antes se normalizaban según las disposiciones de la Ley de Buros de Información Crediticia[116]. Las reformas introducidas en 2012 a esta Ley permitieron determinar la naturaleza de los registros de datos crediticios, el órgano regulador de dichos datos, así como la definición de conceptos fundamentales relacionados con el tratamiento de la información. Sobre esta cuestión, esta Ley expone que:

> Se crea el Registro de Datos Crediticios, con la finalidad de prestar el servicio de referencias crediticias, basado en el análisis de historial de cumplimiento de obligaciones de carácter crediticio de las personas. Este registro permitirá contar con información individualizada de las personas naturales y jurídicas respecto de sus operaciones crediticias que se hayan contratado con las instituciones del sistema financiero público y privado, incluyendo los casos en que éstas actúen en su nombre o por cuenta de una institución bancaria o financiera del exterior, así como de aquellas realizadas con las instituciones del sector financiero popular y solidario, del sector comercial y de otras instituciones en las que se registren obligaciones de pago, las mismas que serán determinadas por resolución de la Dirección Nacional de Registros Públicos.

[114] Carolina Reyes Kahansky, "El deber de notificar y el derecho a la no inculpación en la protección de datos personales", *UNED: Revista de Derecho,* Nro. 24 (2019), 281-318.
[115] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 269.
[116] Esta previsión fue agregada, mediante reforma a la Ley del Sistema Nacional de Registros Públicos. Los artículos normalizados fueron agregados por la Ley Nro. 00, publicada en Registro Oficial Suplemento 843 de 3 de diciembre de 2012.

En relación a la institución encargada de administrar la información proveniente de la solvencia patrimonial y de crédito, dicha norma establece que la Dirección Nacional de Registros Públicos “es la única institución que puede recopilar y mantener la información crediticia proveniente de las fuentes de información de acuerdo a las políticas y formas que establezca para cada sector”. Así también entre las definiciones relativas a las libertades que se puede ejercer, por medio del derecho a la protección de datos, se encuentran las fuentes de la información, información prohibida, bases de datos crediticios e información del registro crediticio. Por su importancia, a continuación, citamos textualmente, el contenido de dichas definiciones:

> Fuentes de Información. - Son las personas, naturales o jurídicas, legalmente autorizadas que, debido a sus actividades, mantienen información crediticia lícita y que tienen la obligación de entregar la misma al Registro Crediticio de conformidad con las políticas y formas que establezca su respectivo organismo de control.
> Información Prohibida. - Es aquella constante en el artículo 6 de la presente Ley y que no podrá ser incluida en el Registro de Datos Crediticios.
> Base de Datos Crediticios. - Es el conjunto de información constante en las bases de datos del registro crediticio proporcionadas por las entidades del sistema financiero público y privado, entidades de la economía popular y solidaria y compañías reguladas por la Superintendencia de Bancos y Seguros, Superintendencia de la Economía Popular y Solidaria; y Superintendencia de Compañías, respectivamente. Información que debe cumplir con las políticas y parámetros que para cada caso las entidades de control determinen.
> Información del Registro Crediticio. - Es el historial crediticio y de cumplimiento de obligaciones: financieras, comerciales, contractuales, de seguros privados y de seguridad social, de una persona natural o jurídica, pública o privada, que sirve para identificarla adecuadamente y determinar sus niveles de endeudamiento.

Con estricta observancia del derecho a la protección de datos personales, observamos que la normativa expuesta está encaminada a garantizar y establecer los mecanismos necesarios para salvaguardar la información personal de los usuarios del sistema crediticio, frente a la posible intervención de terceros. Una muestra de esto, por una parte, es la protección de los datos sensibles, bajo el principio de confidencialidad previsto en el art. 6 de la Ley del Sistema Nacional de Registros Públicos. Y por otra, la garantía que dicha Ley manifiesta sobre el manejo de la información crediticia, la cual “tendrá por exclusiva finalidad el ser destinada a la prestación del servicio de referencias crediticias”.

Como hemos indicado, la protección de la información de carácter personal supone garantizar el derecho al control de los datos y esto, además, implica posibilitar el ejercicio de los derechos de acceso, rectificación y cancelación sobre sus datos personales. En este sentido, precisamos que esta Ley reconoce que el titular de la información crediticia tendrá el derecho a "exigir de la fuente de información crediticia, la rectificación de la información ilegal, inexacta o errónea". Tomando en cuenta que, además, debe adoptarse un nivel más alto de protección, frente a posibles perjuicios materiales[117], la Ley del Sistema Nacional de Registros Públicos determina que todas las bases de datos informáticas deberán "contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impidan la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública" –art. 26–.

En todo caso, entendiendo que "los riesgos que pueden resultar para los derechos y libertades de las personas por las violaciones de la seguridad de los datos son muy variados y dependen en gran medida de la naturaleza de los datos que se están tratando"[118]; esta disposición tan solo hace referencia a las afectaciones sobre la información pública. Por tanto, advertimos la ausencia de garantías de seguridad, específicamente, relacionadas con el tratamiento de la información sobre solvencia patrimonial y de crédito. Finalmente, en relación a la garantía del deber de secreto sobre los reportes crediticios, la Ley en referencia determina que se deberá "obligatoriamente guardar confidencialidad sobre la información contenida en ellos, siendo prohibido utilizarla para fines distintos del análisis crediticio".

En este sentido, recalcamos la importancia de estas prescripciones relacionadas con el tratamiento de la información personal en el ámbito de los datos financieros o bancarios. Si bien, la LOPD determina que los datos crediticios "pueden ser utilizados solamente para esa finalidad y no serán comunicados o difundidos, ni

[117] En este aspecto, la Guía Legislativa de la OEA precisa que los datos personales "deben protegerse, independientemente de la forma en que se mantengan, por medio de salvaguardias razonablemente concebidas para prevenir que las personas sufran daños considerables como consecuencia del acceso no autorizado a los datos o de su pérdida o destrucción".
[118] Reyes Kahansky, "El deber de notificar y el derecho a la no inculpación en la protección de datos personales", 289.

podrán tener cualquier finalidad secundaria" –art. 28–; recordemos que el marco constitucional ecuatoriano exige aplicar a la Constitución como una regla de decisión y, en suma, interpretar la normativa que más favorezca a la efectiva vigencia del derecho a la protección de datos personales. En todo caso, la nueva normativa de protección de datos obliga a que los datos crediticios se deben sujetar a lo previsto en dicha Ley, en la legislación especializada y, en las demás disposiciones que dicte la autoridad de control.

### 2.8 Especial referencia a la protección de datos personales en la Administración pública: Ley del Sistema Nacional de Registros Públicos, Ley Orgánica de Comunicación y Ley Orgánica de Telecomunicaciones

Hemos dejado para el final tres de las normas que mejor han desarrollado en el ámbito sectorial el derecho fundamental a la protección de datos personales.

Por una parte, la promulgación de la Ley del Sistema Nacional de Registros Públicos en 2010, poco a poco está dando los resultados esperados. Aunque su naturaleza, finalidad y objeto no sea, propiamente, desarrollar el contenido del derecho a la protección de datos, esta normativa vincula significativos principios que deben observarse, dentro del marco de protección de la información personal. A esto se suma, la actividad desarrollada por la Dirección Nacional de Registros Públicos, para la tutela de este derecho fundamental, por cuanto tiene como uno de sus principales ejes el control de los registros público, tanto en el ámbito público y privado[119].

[119] En la actualidad, el Ministerio de Telecomunicaciones y Sociedad de la Información –MINTEL–, a través de la Dirección Nacional de Registros Públicos –DINARDAP– ha desarrollado algunas actividades relacionadas con la promoción y necesidad de contar con una legislación para la protección de datos. Precisamente, a inicios de 2018, el MINTEL organizó varias mesas de trabajo para la construcción del Plan de la Sociedad de la Información y del Conocimiento –PSIC–, en donde se incluyeron temas relativos a la protección de la información de carácter personal. Así, el eje 5 de dicha agenda comprendió a la "protección de datos personales", con enfoques hacia los ciudadanos, las empresas y el gobierno. Por otra parte, el MINTEL, con el objeto de desarrollar estrategias y acciones que permitan enfrentar los riesgos que suponen las tecnologías de la información y

Y por otra, la Ley Orgánica de Comunicación amparada, inicialmente, en una serie de normas deontológicas ha considerado exigible a personas naturales y jurídicas la protección y respeto de la intimidad personal. Así también la Ley Orgánica de Telecomunicaciones, que tiene por objeto desarrollar el régimen general de telecomunicaciones, regula y reconoce los principios y derechos constitucionales que se derivan del uso de las telecomunicaciones. Igualmente, el Reglamento de esta última Ley está orientado a establecer las medidas necesarias para la garantía del derecho a la protección de datos.

De esta manera, en los siguientes apartados finales analizaremos las disposiciones relativas a este derecho fundamental y, en algunos casos, las resoluciones y jurisprudencia desarrolladas para la interpretación de las facultades que comprende su ejercicio.

### A. Ley del Sistema Nacional de Registros Públicos

La Ley del Sistema Nacional de Registros Públicos tiene como finalidad "regular el sistema de registros públicos y su acceso, en entidades públicas o privadas que administren dichas bases o registros" –art. 1–, y por objeto "garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información, así como: la eficacia y eficiencia de su manejo, su publicidad, transparencia, acceso e implementación de nuevas tecnologías" –art. 1–[120].

Si bien el ámbito de esta Ley no precisa el contenido del derecho a la protección de datos, sus disposiciones se dedican a establecer un marco jurídico de regulación, sobre la administración de bases o registros de datos públicos que obran en las

comunicación, publicó el" Libro blanco de la Sociedad de la información y del Conocimiento". Entre las temáticas que se abordan en esta obra se encuentran la seguridad de la información; la protección de datos personales y el uso responsable de las Tics.

[120] La Ley del Sistema Nacional de Registros Públicos se aprobó, mediante la Ley Nro. 0 y fue publicada en el Registro Oficial Suplemento Nro. 162 el 31 de marzo de 2010. Debe señalarse que esta Ley ha sido afectada, principalmente, por la Ley Orgánica de Protección de Datos Personales, la cual ha entrado en vigencia en mayo de 2021.

instituciones del sector público y privado –art. 2–[121]. No obstante, en la exposición de motivos, esta Ley determina que, en el contexto del tratamiento de la información, en instituciones públicas o privadas, debe asegurarse el derecho a la protección de datos y la garantía del *habeas data*. En todo caso, a partir de los principios de accesibilidad y confidencialidad –contenidos en el art. 6– se manifiesta que el tratamiento de datos, sometidos a este ámbito, deberá realizarse "conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales".

Ahora bien, en cuanto a la responsabilidad por la administración y tratamiento de la información que obre en dichas bases o registros, el art. 4 de esta Ley precisa que:

> Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información. Las personas afectadas por información falsa o imprecisa, difundida o certificada por registradoras o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal. La Dirección Nacional de Registros Públicos establecerá los casos en los que deba rendirse caución.

Sobre los derechos de accesibilidad y principio de regulación de los datos personales, el art. 6 dispone que:

> Son confidenciales los datos de carácter personal. El acceso a estos datos, solo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales. Al amparo de esta Ley, para acceder a la información sobre el patrimonio de las personas cualquier solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará del mismo y consignar sus datos básicos de identidad, tales como nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el titular de la información pueda ejercer. La Directora o Director Nacional de Registros Públicos, definirá los demás datos que integran el sistema nacional y el tipo de reserva y accesibilidad.

[121] No obstante, es conveniente subrayar que en la exposición de motivos de esta Ley se expresa la importancia del respeto del derecho a la protección de datos, así como de la garantía jurisdiccional del *habeas data*.

Esta Ley estableció la creación de la Dirección Nacional de Registros Públicos como un organismo de derecho público –con autonomía administrativa, técnica, operativa, financiera y presupuestaria, adscrita al Ministerio de Telecomunicaciones y Sociedad de la Información–, con jurisdicción en todo el Estado. Conforme en lo dispuesto por el art. 31 de dicha Ley, entre sus principales atribuciones y facultades se encuentra:

a. Dictar las resoluciones y normas necesarias para la organización y funcionamiento del sistema;
b. Promover, dictar y ejecutar a través de los diferentes registros, las políticas públicas a las que se refiere esta Ley, así como normas generales para el seguimiento y control de las mismas;
c. Definir los programas informáticos y los demás aspectos técnicos que todas las dependencias de registros públicos deberán implementar para el sistema interconectado y control cruzado de datos, y mantenerlo en correcto funcionamiento;
d. Vigilar y controlar la correcta administración de la actividad registral;
e. Sancionar de conformidad con la Ley que regula a la servidora o servidor público, el incumplimiento de los deberes y obligaciones de las registradoras o registradores;
f. Promover, organizar y ejecutar programas de capacitación de las registradoras o registradores públicos y demás personal de los registros.

Además, debido a la promulgación de la LOPD, se han agregado otras dos atribuciones relacionadas con:

1. Controlar y supervisar que las entidades pertenecientes al Sistema Nacional de Registros Públicos incorporen mecanismos de protección de datos personales, así como dar cumplimiento a las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación y demás normativa que la Autoridad de Protección de Datos Personales dicte para el efecto; y
2. Tratar datos procedentes del Sistema Nacional de Registros Públicos o de cualquier otra fuente, para realizar procesos de analítica de datos, con el objeto de prestar servicios al sector público, al sector privado y a personas en general, así como generar productos, reportes, informes o estudios, entre otros. Se utilizarán medidas adecuadas que garanticen el derecho a la protección de datos personales y su uso en todas las etapas del tratamiento, como, por ejemplo, técnicas de disociación de datos

Por otra parte, el Reglamento de la Ley del Sistema Nacional de Registros Públicos desarrolla de manera más específica las atribuciones de regulación y control de la Dirección Nacional de Registros Públicos[122]. En este caso, el art. 9 del Reglamento determina que:

[122] El Reglamento de la Ley del Sistema Nacional de Registro de Datos Públicos se aprobó, mediante el Decreto Ejecutivo Nro. 950 y fue publicada en el Registro Oficial Suplemento Nro. 718 el 23 de marzo de 2016.

> Sin perjuicio de las competencias que ejercen los entes de control, definidos en la Constitución de la República, la Dirección Nacional de Registros Públicos es el órgano de regulación, control, auditoría y vigilancia de todos los integrantes del Sistema Nacional de Registros Públicos en torno a la interoperabilidad de datos. La regulación, control, auditoría y vigilancia comprenden todas las acciones necesarias para garantizar la disponibilidad del servicio. Las decisiones administrativas internas de cada ente registral corresponden exclusivamente a sus autoridades, pero la Dirección Nacional de Registros Públicos arbitrará las medidas que sean del caso cuando perjudiquen la disponibilidad de los servicios.

El Reglamento también señala los principios que deben observarse en el tratamiento de la información en las bases de datos y registros que se encuentran bajo la administración del Sistema Nacional de Registros Públicos. De esta manera, el art. 11 del Reglamento reconoce que, en el ámbito público y privado se deberán observar los siguientes principios:

> 1. Principio de veracidad o calidad de los datos personales. - La información contenida en los registros o bases de datos públicos o privados debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
> 2. Principio de finalidad. - El tratamiento de datos personales debe responder a una finalidad legítima, de acuerdo a la Constitución de la República y la Ley.
> 3. Principio de utilidad. - El acopio, procesamiento y divulgación de los datos personales deben cumplir una función determinada que sirva a la finalidad que persiga el registro del dato.
> 4. Principio de incorporación. - Cuando de la inclusión de datos personales en determinadas bases se deriven situaciones ventajosas para el titular, la entidad administradora de datos estará en la obligación de incorporarlos, si el titular reúne los requisitos que el orden jurídico exige para tales efectos, de tal forma que queda prohibida negar la incorporación injustificada a la base de datos.
> 5. Principio de rectificabilidad. - Los datos públicos registrados son susceptibles de rectificación o supresión en los casos y con los requisitos previstos por la Ley y el presente Reglamento.
> 6. Principio de responsabilidad. - La responsabilidad sobre la veracidad y autenticidad de los datos registrales, es responsabilidad del declarante, cuando éste provea la información; sin perjuicio de los mecanismos de verificación que implemente la Institución ante quien se efectúe la declaración.

Por otra parte, sobre el ejercicio de los derechos ARCO, el art. 12 del Reglamento tutela el ejercicio del derecho a la rectificación, actualización, eliminación y anulación de datos, señalando que:

> Sin perjuicio de las demás acciones previstas en el ordenamiento jurídico, toda rectificación, actualización o eliminación de los datos que consten en los registros públicos únicamente podrá ser solicitada por el titular de los mismos, quien deberá presentar los documentos que justifiquen la modificación exigida. La solicitud deberá presentarse directamente a la entidad de la que provenga el dato cuyo cambio se exige. La entidad a la que se solicite la rectificación, actualización o eliminación, sea ésta pública o privada, deberá atender la solicitud en un plazo máximo de 15 días. La negativa deberá estar debidamente fundamentada con los argumentos de hecho y de derecho que corresponda. La Dirección Nacional de Registros Públicos no podrá, por sí misma, rectificar, actualizar, eliminar o anular ningún dato; únicamente lo hará cuando el registro público correspondiente lo haya hecho previamente y luego de las verificaciones que correspondan. No obstante, lo antes

> mencionado, las actualizaciones de los datos podrán realizarse de manera directa por parte de los registros públicos, cuando éstos actúen en uso de sus atribuciones legales, y siempre que puedan demostrar, con documentos oficiales o declaraciones de los titulares de los datos, la actualización realizada. Mientras esté en curso una petición de rectificación, actualización o eliminación, la entidad responsable del tratamiento de los datos públicos deberá hacer constar dicho particular en los documentos que emita en relación con la información sujeta a rectificación.

Observamos que esta Ley garantiza el ejercicio de los derechos "ARCO" dentro del tratamiento de la información personal. Así, la administración sujeta a la regulación de esta norma, tiene la obligación de conceder el acceso a la información personal que se encuentre contendida en bases de datos, incluyendo éstas en el ámbito privado. Además, para el caso de que la información sea equívoca –errónea o inexacta– se garantiza los derechos de rectificación, actualización o eliminación de la información. En este sentido, la protección de la información personal en la administración de las bases de datos o registros tiene que desarrollarse atendiendo los principios que han quedado anotados. Principalmente, por el principio de finalidad por el que la información es almacenada.

### B. Ley Orgánica de Comunicación

Como hemos precisado, la protección de datos se encuentra muy vinculada al desarrollo de las tecnologías de la información y comunicación. "Los avances sufridos en el terreno de los medios de comunicación, en concreto, en el sector televisivo -y no sólo en cuanto a su forma, sino especialmente en cuanto a su contenido- han influido profundamente en la percepción que los ciudadanos tienen de este nuevo derecho"[123]. En este orden de ideas, otra norma promulgada para salvaguardar el derecho a la protección de datos, en el ámbito de los medios de comunicación, es la Ley Orgánica de Comunicación –en adelante LOC–[124], por cuanto –atendiendo el mandato constitucional previsto en el art. 11.3– determina

[123] Mónica Arenas Ramiro, "El valor de la información personal: Protección de datos personales y la sociedad del espectáculo", Anuario Facultad de Derecho – Universidad de Alcalá, Nro. 2 (2009) 275-300.
[124] La Ley Orgánica de Comunicación se aprobó, mediante Ley Nro. 0 y fue publicada en el Registro Oficial Suplemento Nro. 22 el 25 de junio de 2013.

que “los derechos y garantías establecidos en los instrumentos internacionales ratificados por el Ecuador, la Constitución o la presente Ley serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial de oficio o a petición de parte” –art. 2–[125].

Dentro del tipo de información restringida que no pueden divulgarse o circular en los medios de comunicación, encontramos aquella “protegida expresamente en la Ley” –art. 30–[126]. En un sentido amplio, se hace referencia a la información de carácter personal tutelada, a través del derecho fundamental a la protección de datos personales y la garantía del *habeas data*. Así, por ejemplo, entendemos que “la reproducción o publicación de la imagen de las personas sin su consentimiento, cuando no se están desarrollando acciones que cabría calificar de intimas, merecen el reproche del ordenamiento”[127]. Por tanto, si bien es “en el terreno de la comunicación donde se produce una colisión evidente entre el derecho a la protección de datos personales y la libertad de expresión ejercida a través de estos medios”[128]; esto obliga a establecer unos juicios de proporcionalidad y de ponderación cuando estos derechos entren en conflicto, por cuanto la LOPD manifiesta que “los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión estarán

[125] Hay que anotar que, antes de la reforma publicada en Registro Oficial Suplemento Nro. 432 de 20 de febrero de 2019, la LOC, en su art. 10 establecía una serie de normas deontológicas encaminadas, por ejemplo, a observar el respeto de la dignidad humana, la honra y la reputación de las personas, la intimidad personal y familiar. Así también el deber de proteger el derecho a la imagen y privacidad de adolescentes en conflicto con la Ley penal.

[126] Este artículo fue sustituido por el artículo 23 de Ley No. 0, publicada en Registro Oficial Suplemento Nro. 432 de 20 de febrero de 2019. En este sentido, anterior a esta reforma, esta disposición consideraba como información restringida: “aquella que esté protegida expresamente con una cláusula de reserva previamente establecida en la Ley” –art. 30.1–; la información “acerca de datos personales y la que provenga de las comunicaciones personales, cuya difusión no ha sido debidamente autorizada por su titular, por la Ley o por juez competente” –art. 30.2–; la “producida por la Fiscalía en el marco de una indagación previa” –art. 30.3–; y la información “acerca de las niñas, niños y adolescentes que viole sus derechos según lo establecido en el Código de la Niñez y Adolescencia” –art. 30.4–.

[127] Esperanza Gómez Corona, “Derecho a la propia imagen, nuevas tecnologías e Internet”, en Lorenzo Cotino Hueso (Ed.), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*. Valencia. Universidad de Valencia. 2011. 444-466.

[128] Arenas Ramiro, “El valor de la información personal: Protección de datos personales y la sociedad del espectáculo”, 281.

sujetos a los principios establecidos en esta Ley, en los casos que corresponda y sea de aplicación favorable" –art. 11–.

Por otra parte, sobre el derecho a la protección de las comunicaciones personales, el art. 31 de la LOC prevé que:

> Todas las personas tienen derecho a la inviolabilidad y al secreto de sus comunicaciones personales, ya sea que éstas se hayan realizado verbalmente, a través de las redes y servicios de telecomunicaciones legalmente autorizadas o estén soportadas en papel o dispositivos de almacenamiento electrónico. Queda prohibido grabar o registrar por cualquier medio las comunicaciones personales de terceros sin que ellos hayan conocido y autorizado dicha grabación o registro, salvo el caso de las investigaciones encubiertas autorizadas y ordenadas por un juez competente y ejecutadas de acuerdo a la Ley. La violación de este derecho será sancionada de acuerdo a la Ley.

Es conveniente destacar que, a la luz del art. 2 y art. 30 de la LOC, se desprende la relevancia del respeto del principio de consentimiento, en el tratamiento de la información personal, tanto en lo relacionado a la circulación de la información como en la regulación del derecho de protección de las comunicaciones personales. "En todo caso y, dada la virtualidad del consentimiento en este punto, lo único que cabe hacer es analizar caso por caso, en orden a constatar si ese consentimiento ha existido"[129]. En este sentido, si esta comunicación "cuenta con el consentimiento del sujeto, el tratamiento de sus datos personales –la difusión de su información por los medios de comunicación– cumpliría con los requisitos de licitud"[130].

Como hemos advertido, el ejercicio de los derechos de comunicación, entre otros, comprende derechos incardinados con la libertad de expresión, y que, incuestionablemente, pueden afectar el derecho a la protección de datos personales. Desde esta perspectiva, sobre la naturaleza del derecho a la libertad de expresión, la CCE en la Resolución 2 –Caso signado con el Nro. 6-10/IA– apunta que:

> El derecho constitucional a la libertad de expresión es un derecho que encuentra sus límites razonables en los derechos de los demás (…) Asumir que el derecho a la libertad de expresión y opinión es un derecho absoluto y que por lo tanto, no existe ningún límite racional a su ejercicio, resulta un equívoco, dado que el ejercicio de todo derecho encuentra su límite en los derechos de las demás personas (…) Por lo tanto, el ejercicio del derecho a la libertad

[129] Gómez Corona, "Derecho a la propia imagen, nuevas tecnologías e Internet", 457.
[130] Arenas Ramiro, "El valor de la información personal: Protección de datos personales y la sociedad del espectáculo", 285.

> de expresión y de opinión no es un derecho absoluto, tiene que necesariamente desarrollarse en respeto y salvaguarda de los demás derechos constitucionales.

La misma Resolución, en relación a las posibles intromisiones que los medios de comunicación pueden producir en el ejercicio de su actividad, explica que:

> En estos casos, el ordenamiento jurídico debe proveer a quien se considere afectado los mecanismos más apropiados para garantizar un equilibrio entre el ejercicio legítimo del derecho a la comunicación mediante información u opinión en medios de comunicación, y la salvaguarda de otros derechos establecidos en la Constitución y en tratados internacionales de derechos humanos, tales como el honor y el buen nombre así como la protección de la seguridad nacional (…) No obstante, tal como ha reiterado esta Corte Constitucional, los derechos tienen limitaciones, pues no son absolutos, y la limitación a los derechos a la comunicación e información tiene un sustento razonable y justificable cuando se pretende el ejercicio de otros derechos, sin que ello signifique la imposición de unos sobre otros; es decir, lo que pretende la regulación es que los derechos se ejerzan de forma coordinada, guardando la debida armonía para su perfecto desarrollo (…) Los medios de comunicación tienen el deber jurídico de enmarcar su actuación en la esfera del respeto a los derechos constitucionales de las personas, pues lo contrario evidenciaría un ejercicio abusivo de la libertad de expresión y la inadecuada prestación del servicio de comunicación.

En este punto, precisamos las siguientes reflexiones. Primero, en la LOC, la garantía del derecho a la protección de los datos se enmarca en el principio constitucional de eficacia directa, reconocido en el art. 2 de dicha Ley. Segundo, reconociendo que "la información sobre comportamientos, gustos y actividades personales se ha convertido en una de las mercancías más preciadas por las empresas, las cuales necesitan información para poder actuar en el tráfico jurídico"[131], el ejercicio de la libertad de expresión en los medios de comunicación debe orientarse a adoptar las medidas necesarias, que permitan una adecuada protección jurídica de la información. Y tercero, la reforma introducida en 2019 es cuestionable, en lo relativo a la eliminación de las normas deontológicas, toda vez que, muchas de las intromisiones en la vida privada de las personas, producto del ejercicio de la libertad de expresión de los medios de comunicación, surgen como resultado de la inobservancia de reglas morales y éticas.

### C. Ley Orgánica de Telecomunicaciones

[131] Ibíd., 286.

Como hemos destacado, en razón del avance tecnológico pueden ser innumerables las intromisiones arbitrarias e ilegítimas en la vida privada de las personas, las cuales pueden, en suma, afectar el derecho a la protección de datos. En la era de las tecnologías, "los medios utilizados para el tránsito de información son las redes de telecomunicaciones. Como ejes centrales o cables que forman parte de Internet y por las cuales pasan las comunicaciones en la red desde el punto de expedición hasta el punto de destino"[132]. Por tanto, conviene analizar la regulación que existe en este ámbito, a la luz de los presupuestos que comprende este derecho fundamental.

El ordenamiento jurídico ecuatoriano sobre protección de datos evidencia dos etapas, plenamente, diferenciadas cuyo vértice es, sin duda, la inclusión de la protección constitucional de la información de carácter personal. En este marco, uno de los principales problemas que evidenciamos es la ausencia de garantías mínimas de seguridad que resulten aplicables al tratamiento de la información. No obstante, la Ley Orgánica de Telecomunicaciones reconoce trascendentales disposiciones que desarrollan el contenido y protección de este fundamental[133].

Por ejemplo, sobre las obligaciones de los prestadores de servicios de telecomunicaciones, dicha Ley establece que es obligación "adoptar las medidas necesarias para la protección de los datos personales de sus usuarios y abonados, de conformidad con esta Ley, su Reglamento General y las normas técnicas y regulaciones respectivas" –art. 24.14–. En cuanto a las medidas técnicas de seguridad e invulnerabilidad, el art. 76 determina que:

> Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la

[132] José López Calvo, "Un Reglamento poliédrico que necesita un acercamiento poliédrico", en José López Calvo (coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*. Madrid. Wolters Kluwer. 2018, 89.

[133] La Ley Orgánica de Telecomunicaciones se aprobó, mediante Ley Nro. 0 y fue publicada en el Registro Oficial 439 el 18 de febrero de 2015. Respecto a la importancia de la regulación del tratamiento de la información en el sector de las telecomunicaciones, imaginemos "que mediante dispositivos de radiofrecuencia es posible no solo controlar las ventas en un centro comercial sino también localizar las personas". Cfr. Lucas Murillo de la Cueva y Piñar, El *derecho a la autodeterminación informativa*, 142. Por ello, al igual que la Ley del Sistema Nacional de Registros Públicos, la Ley Orgánica de Telecomunicaciones ha sido reformada en varios artículos por la LOPD.

> información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente. En caso de que exista un riesgo particular de violación de la seguridad de la red, el prestador de servicios de telecomunicaciones deberá informar a sus abonados, clientes o usuarios sobre dicho riesgo y, si las medidas para atenuar o eliminar ese riesgo no están bajo su control, sobre las posibles soluciones.

En lo relacionado a la interceptación de las comunicaciones personales, el art. 77 manifiesta que:

> En caso de interceptación legal, las y los prestadores de servicios deberán proveer toda la información requerida en la orden de interceptación, incluso los datos de carácter personal de los involucrados en la comunicación, así como la información técnica necesaria y los procedimientos para la descompresión, descifrado o decodificación en caso de que las comunicaciones objeto de la interceptación legal hayan estado sujetas a tales medidas de seguridad. Los contenidos de las comunicaciones y los datos personales que se obtengan como resultado de una orden de interceptación legal estarán sujetos a los protocolos y reglas de confidencialidad que establezca el ordenamiento jurídico vigente.

Así también como parte de las reformas que introdujo la LOPD, el art. 78 reconoce la garantía de la seguridad de los datos personales, señalando la obligación de adoptar "medidas técnicas, organizativas y de cualquier otra índole adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos personales de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales". Por otra parte, el art. 79 de dicha Ley –también reformado por la nueva normativa de protección de datos– advierte la importancia del deber de información, como necesario para notificar al titular de este derecho. En lo pertinente, esta disposición precisa que "en caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de telecomunicaciones, el prestador de servicios de telecomunicaciones informará a sus abonados, clientes y usuarios sobre dicho riesgo y sobre las medidas a adoptar".

Ahora bien, la LOPD ha introducido en el art. 81 de la Ley Orgánica de Telecomunicaciones el derecho al titular de los datos:

> A no figurar en guías telefónicas o de abonados. Deberán ser informados, de conformidad con lo establecido en la Ley Orgánica de Protección de Dalos Personales, de sus derechos con respecte a la utilización de sus datos personales en las guías telefónicas o de abonados y, en particular, sobre el fin o los fines de dichas guías, así como sobre el derecho que tienen, en forma gratuita, a no ser incluidos, en tales guías.

Además, con referencia a las mencionadas reformas, el art. 82 regula el uso comercial de datos personales. Así, dispone que:

> Las y los prestadores de servicios no podrán usar datos personales, información del uso del servicio, información de tráfico o el patrón de consumo de sus abonados, clientes o usuarios para la promoción comercial de servicios o productos, a menos que el abonado o usuario al que se refieran los datos o tal información, haya dado su consentimiento conforme le establecido en la Ley Orgánica de Protección de Datos Personales. Los usuarios o abonados dispondrán de la posibilidad clara y fácil de retirar su consentimiento para el uso de sus datos y de la información antes indicada. Tal consentimiento deberá especificar los datos personales o información cuyo uso se autorizan, el tiempo y su objetivo específico. Sin contar con tal consentimiento y con las mismas características, las y los prestadores de servicios de telecomunicaciones no podrán comercializar, ceder o transferir a terceros los datos personajes de sus usuarios, clientes o abonados. Igual requisito se aplicará para la información del uso del servicio, información de tráfico o del patrón de consumo de sus usuarios, clientes y abonados.

Desde este ámbito, se han delegado facultades a la Agencia de Regulación y Control de las Telecomunicaciones en lo relacionado a los mecanismos de supervisión, para el secreto de las telecomunicaciones y seguridad de datos personales. Así, el art. 85 de la Ley establece que:

> La Agencia de Regulación y Control de las Telecomunicación establecerá y reglamentará los mecanismos para supervisar el cumplimiento de las obligaciones tanto de secreto de las comunicaciones y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para las y los prestadores de servicios, con el fin de que adopten determinadas medidas relativas a la integridad y seguridad de las redes y servicios. Entre ellas, podrá imponer: 1. La obligación de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad; 2. La obligación de someterse a costo del prestador, a una auditoría de seguridad realizada por un organismo público, autoridad competente o, de ser el caso, por una empresa privada o persona natural independiente.

Como hemos analizado en otro momento, uno de los requerimientos necesarios en toda legislación de protección de datos es la autoridad de control. En el presente caso, según el Reglamento General a la Ley Orgánica de Telecomunicaciones la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) es uno de los organismos competentes dentro del régimen de telecomunicaciones –art. 4–. La máxima autoridad es el Director Ejecutivo –art. 6–, con capacidad para emitir actos administrativos y normativos –art. 9–. Si bien, en sus funciones no se estima referencia específica a desarrollar actividades de supervisión y control en el marco de protección de datos; a partir de lo dispuesto en el Reglamento, la ARCOTEL puede ejercer otras funciones previstas en el Reglamento General –art. 9.7–. Por tanto, consideramos que, conforme lo dispone el art. 85, también se encontraría habilitada para ejercer actividades de control y supervisión sobre el marco de protección de datos personales.

De esta manera, subrayamos que uno de los principios que enmarca el funcionamiento y ejercicio de las autoridades de control es el principio de independencia funcional. Como prevé el Reglamento "los actos administrativos y normativos que emita el Director Ejecutivo, podrán ser impugnados únicamente ante el mismo órgano, dicha resolución pondrá fin a la vía administrativa" –art. 6–. En todo caso, sus resoluciones se caracterizan por estar exentas de influencia de terceros. Puede decirse, entonces, que ARCOTEL tiene la calidad de autoridad de control, aunque limitada en cuanto a sus funciones.

En otro orden de ideas, apreciamos que el Reglamento General a la Ley Orgánica de Telecomunicaciones complementa la regulación de la Ley general en lo relativo a la protección de datos personales[134]. En este aspecto, el art. 120 del Reglamento dispone que:

> Los prestadores de servicios del régimen general de telecomunicaciones tienen prohibido ejecutar u omitir acciones que violen la garantía de protección de datos personales, esto es, provocar la destrucción, la pérdida, la alteración, la revelación o el acceso no autorizado de datos personales, transmitidos, almacenados o tratados en la prestación de servicios de telecomunicaciones, conforme el alcance, los procedimientos o protocolos previstos en la LOT, su Reglamento General y las regulaciones emitidas por la ARCOTEL para el efecto. La violación de esta garantía dará lugar a la imposición de las sanciones previstas en el ordenamiento jurídico.

Es evidente que esta norma garantiza la inviolabilidad y el secreto de la información y las comunicaciones transmitidas, a través de medios telemáticos; y desde luego, concreta el respeto a la garantía de protección de los datos personales, por parte de los prestadores de servicios. Por ello, corresponde advertir que las tecnologías "se convierten en los guardabarreras que modulan cuando suministran incluso a las autoridades policiales la ingente información sobre las personas que contienen sus servidores y cuando no. Depositarias de nuestra identidad digital —con la que podemos a veces no reconocernos— cuyos rasgos como un «me gusta» en *Facebook* sirve hasta para denegar créditos"[135].

[134] El Reglamento General a la Ley Orgánica de Telecomunicaciones se aprobó mediante Decreto Ejecutivo Nro. 864 y fue publicada en el Registro Oficial Suplemento 676 el 25 de enero de 2016.
[135] López Calvo, "Un Reglamento poliédrico que necesita un acercamiento poliédrico", en José López Calvo (coord.), 85.

Finalmente, destacamos que otra de las problemáticas del derecho a la autodeterminación informativa, es el uso comercial de los datos personales. Con referencia a este aspecto, puede atribuirse, tanto a la Ley Orgánica de Telecomunicaciones como a su Reglamento ser la primera norma que regula el uso comercial de la información de carácter personal. En este caso, el art. 121 del Reglamento determina que:

> Los datos personales que los usuarios proporcionen a los prestadores de servicios del régimen general de telecomunicaciones no podrán ser usados para la promoción comercial de servicios o productos, inclusive de la propia operadora; salvo autorización y consentimiento expreso del usuario. Para tal fin, los prestadores de servicios deberán solicitar a sus usuarios su consentimiento expreso, en un instrumento separado y distinto al contrato de prestación de servicios a través de medios físicos o electrónicos, para que la prestadora de servicios del régimen general de telecomunicaciones pueda utilizar comercialmente sus datos personales. En dicho instrumento se deberá dejar constancia expresa de los datos personales o información que están expresamente autorizados; el plazo de la autorización y el objetivo que esta utilización persigue. Sin perjuicio de lo anterior se considerarán públicos los datos contenidos en las guías telefónicas de telefonía fija, no obstante, lo cual los abonados tendrán derecho a que se excluyan gratuitamente sus datos personales de dichas guías. La ARCOTEL establecerá los mecanismos y emitirá las regulaciones correspondientes a fin de precautelar el secreto de las comunicaciones y de la información que se trasmite a través de redes de telecomunicaciones, así como la seguridad de los datos personales y de las redes.

Cada vez son mayores las intromisiones relacionadas con la apropiación de la información de carácter personal, con el objeto de obtener algún beneficio de carácter económico. “En las sociedades actuales desarrolladas ha adquirido gran importancia comercial y económica la elaboración de ficheros de datos personales destinados a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas”[136]. Por ello, hay que entender que el sector de las telecomunicaciones desencadena un flujo constante de información, con graves afectaciones en las libertades, que se desprenden del derecho a la protección de datos. Así, por ejemplo:

> La computación en nube, esto es, informática basada en internet en la que los programas, los recursos compartidos y la información se encuentran en servidores remotos, también plantean retos para la protección de datos, dado que puede implicar la pérdida del control por parte de los individuos de su información potencialmente sensible cuando almacenan sus datos utilizando programas alojados en servidores ajenos[137].

[136] Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, 307.
[137] Artemi Rallo Lombarte, “Hacia un nuevo sistema europeo de protección de datos: Las claves de la reforma*”, UNED: Revista de Derecho Político*, Nro. 85 (2012), 13-56.

Tomando en cuenta que, en la actualidad, “los métodos de recogida de los datos personales son cada vez más complicados y se detectan con más dificultad. El mayor recurso a procedimientos que permiten la recogida automática de datos, como el pago electrónico de billetes, el cobro de peajes en carreteras, o instrumentos de geolocalización”[138]; es imprescindible tomar en cuenta la LOPD, por cuanto ésta prescribe medidas jurídicas y técnicas, que desde todos los sectores respeten de manera integral el derecho fundamental a la protección de datos personales y garanticen la confianza y seguridad jurídica de los ciudadanos.

[138] Ibíd., 18.

## CAPÍTULO IV: ANÁLISIS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES EN ECUADOR. REFERENCIAS A LOS PROYECTOS DE LEY DE 2016 Y 2019

### 1. Introducción

En capítulos anteriores, hemos hecho referencia a la naturaleza y el origen del derecho a la protección de datos, tanto en el contexto internacional como en Ecuador. En el ordenamiento jurídico ecuatoriano, el desarrollo de este derecho en la normativa secundaria y/o sectorial constituye una garantía necesaria para el aseguramiento y respeto de la seguridad jurídica y confianza ciudadana. Por ello, a partir de la promulgación de la Ley Orgánica de Protección de Datos personales en Ecuador, en adelante, nos dedicaremos a reflexionar sobre los presupuestos jurídicos necesarios para la fundamentación y aplicación de dicha Ley.

Como hemos precisado, los derechos fundamentales son inherentes a la persona humana, lo cual implica el respeto de la dignidad en todas sus dimensiones. La protección de datos personales conlleva, precisamente, el reconocimiento de derechos y obligaciones solidarias y recíprocas. Su ejercicio conlleva una "colisión con otros derechos fundamentales y bienes constitucionales que implican el conocimiento y acceso a la información personal y el tratamiento de datos personales sin consentimiento"[1]. Autores como Pérez Luño y Antonio Troncoso coinciden en la necesidad de *"*buscar equilibrio*",* desde el ámbito de relación entre la administración y los ciudadanos, en lo que respecta al tratamiento de la información de carácter personal. Este planteamiento sugiere en gran medida la necesidad de un "pacto social*",* que asegure la proporcionalidad de los límites al derecho a la protección de datos personales y a otras libertades fundamentales. En este orden de ideas, advertimos la necesidad de "un adecuado ordenamiento

[1] Antonio Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, (Valencia: Tirant lo Blanch, 2010), 33.

jurídico de la informática, capaz de armonizar las exigencias de información propias de un Estado avanzado con las garantías de los ciudadanos"[2].

El Estado constitucional de derechos y justicia ecuatoriano plantea que –conforme al principio de eficacia directa–, los derechos y garantías reconocidos en la Constitución constituyen una regla de decisión. Las decisiones de los servidores públicos, administrativos o judiciales deben garantizar su aplicación, de manera directa e inmediata. De hecho, "los pretextos de falta de Ley o reglamento para excusarse de cumplir un derecho, tan comunes en un Estado burocratizado, no tienen cabida"[3]. Según este paradigma, en principio, la falta de una Ley general o normas sectoriales, aplicables al tratamiento de la información personal, no puede limitar el ejercicio del derecho a la protección de datos, frente a la actividad de los poderes públicos, incluso particulares. No obstante, hay que recordar que uno de los pilares esenciales para que el tratamiento de la información sea legítimo y respete los derechos y libertades individuales, es la necesidad de garantizar la coherencia –seguridad jurídica– de la legislación nacional.

La protección de datos personales en las sociedades actuales "precisan de un equilibrio entre el flujo de informaciones, que es condición indispensable de una sociedad democrática y exigencia para la actuación eficaz de los poderes públicos, con la garantía de la privacidad de las personas"[4]. Lógicamente, este equilibrio y coherencia se traduce, a su vez, en la garantía del derecho a la seguridad jurídica que –como consagra la Constitución–, "se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes" –art. 82–[5]. Con referencia a esta garantía, la Corte Constitucional de Ecuador determina que:

---

[2] Antonio Pérez Luño, *Derechos Humanos, Estado de Derecho y Constitución*, (Madrid: Tecnos, 2010), 363.

[3] Ramiro Ávila Santamaría, *Los derechos y sus garantías. Ensayos críticos*, (Quito-Ecuador: Corte Constitucional para el Período de Transición, 2012), 77.

[4] Pérez Luño, *Derechos Humanos, Estado de Derecho y Constitución*, 363.

[5] Recordemos que, en ámbito internacional, el Reglamento (UE) 2016/679 pone de manifiesto la necesidad de "reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas" **–**Considerando 7**–**. Precisamente, consideramos que "la

> La seguridad jurídica se constituye en un derecho sustancial dentro del Estado constitucional de derechos y justicia, ya que reafirma como su fundamento principal el respeto a la Constitución, como la máxima norma del ordenamiento jurídico, cuyo respeto se constituye en una obligación del Estado en general y de las autoridades públicas en particular, adicionalmente la seguridad jurídica es una garantía de la certeza jurídica, en tanto determina la obligación de la aplicación de normas jurídicas previas, claras y públicas por parte de las autoridades competentes[6].

Como hemos examinado en otro momento, el desarrollo de este derecho dentro del ordenamiento jurídico secundario es insuficiente. A partir del desarrollo tecnológico, resulta escaso, disperso y limitante a la hora de aplicar los presupuestos, principios y definiciones necesarias en la regulación del tratamiento –automatizado o no– de la información de carácter personal. "La tecnología permite a los ciudadanos intercambiar fácilmente información con respecto a sus comportamientos y sus preferencias, y hacerla pública a nivel mundial a una escala sin precedentes"[7]. Frente a esta situación, la tutela de los derechos fundamentales –especialmente, el de protección de datos personales– precisan una particular atención debido a que, en el contexto jurídico, debe converger la garantía integral de las libertades personales y la confianza ciudadana, con la evolución que plantea el paradigma tecnológico[8].

---

elección del Reglamento como instrumento normativo para reformar el marco general de protección de datos viene a satisfacer de forma muy especial las pretensiones de la segunda estrategia expuesta si bien, al no agotar toda su potencialidad armonizadora, se ubica en una posición intermedia que, en todo caso, busca dar respuesta a la necesidad de seguridad jurídica mediante la global y coherente aplicación de la protección de datos en todo el territorio de la Unión, el efectivo ejercicio de los derechos individuales de protección de los datos y la mejora en su supervisión. Cfr. Artemi Rallo Lombarte, "Hacia un nuevo sistema europeo de protección de datos: Las claves de la reforma*", UNED: Revista de Derecho Político*, Nro. 85 (2012), 13-56.

[6] Véase la Resolución de la Corte Constitucional 287, Sentencia Nro. 287-16-SEP-CC **–**CASO Nro. 578-14-EP**–** publicada en el Registro Oficial Suplemento Nro. 854 de 4 de octubre de 2016.

[7] Rallo Lombarte, "Hacia un nuevo sistema europeo de protección de datos: Las claves de la reforma*", UNED: Revista de Derecho Político*, Nro. 85 (2012), 18.

[8] Sobre este respecto, la Corte Constitucional de Ecuador insiste en que el derecho a la seguridad jurídica "constituye el pilar sobre el cual se asienta la confianza ciudadana respecto de las actuaciones de los poderes públicos, pues brinda a las personas certeza de que la aplicación normativa se realizará acorde a la Constitución y que las normas aplicables al caso concreto han sido determinadas previamente, son claras y públicas, y aplicadas únicamente por autoridad competente. Solo de esta manera se logra conformar una certeza de que la normativa existente en la legislación será aplicada cumpliendo ciertos lineamientos que garantizan el acceso a la justicia y una tutela efectiva, imparcial y expedita de sus derechos e intereses". Véase la Resolución de la Corte Constitucional Nro. 78, Sentencia Nro. 78-15-SEP-CC **–** CASO Nro. 788-14-EP**–** publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015.

Conforme a los presupuestos para la garantía de la seguridad jurídica que plantea la Corte Constitucional de Ecuador –en adelante CCE–, es evidente la necesidad de que la Ley Orgánica de Protección de Datos Personales –en adelante LOPD– asegure, que los tratamientos de la información personal en los distintos sectores se ajusten a unos principios generales. Las autoridades públicas "utilizan cada vez más datos personales con distintos fines: para buscar personas cuando se declara una enfermedad transmisible, para prevenir y luchar más eficazmente contra el terrorismo y la delincuencia, para gestionar su régimen de seguridad social o a efectos fiscales, en el marco de sus aplicaciones de administración en línea, etc."[9]. Por ello, con el objeto de establecer la coherencia, confianza y seguridad jurídica en la legislación, es esencial analizar las facultades, obligaciones y condiciones de legitimación que supone el respeto integral de la normativa de protección de datos.

A partir de las condiciones que plantea la seguridad jurídica, el marco de protección y regulación del derecho a la protección de datos debe orientarse a concretar normas claras y legítimas que, asegurando la confianza ciudadana, respeten de manera integral la Constitución y los principios internacionales para la protección y tutela de la intimidad, privacidad y, en suma, de la información de carácter personal[10]. En todo caso, recordando que este derecho fundamental exige que se "otorgue al individuo las facultades necesarias para que pueda controlar y disponer libremente de sus propios datos personales como garantía última de su dignidad y del libre desarrollo de su personalidad"[11]; el tratamiento de la información debe singularizarse, dentro de un marco jurídico integral y equilibrado, que atribuya al

[9] Rallo Lombarte, "Hacia un nuevo sistema europeo de protección de datos: Las claves de la reforma*", UNED: Revista de Derecho Político*, Nro. 85 (2012), 18.

[10] La Sentencia 182-15-SEP de la CCE advierte que, además, la seguridad jurídica "radica en que las actuaciones de las diversas instituciones y autoridades se fundamenten en normas jurídicas previamente determinadas, aprobadas de manera legítima y pública, y por ende se enmarcan dentro de las normas constitucionales y legales, verificándose de esta manera la validez del actuar de la autoridad. Esta actuación de juridicidad tiene como consecuencia el conocimiento y la confianza que tienen los ciudadanos respecto de que los diferentes aspectos y situaciones de la vida social se encuentran regulados y resueltos por normas y previstas en el ordenamiento jurídico". Véase la Resolución de la Corte Constitucional Nro. 182, Sentencia Nro. 182-15-SEP-CC **–**CASO Nro. 1493-10-EP**–** publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015.

[11] Mónica Arenas Ramiro, "La protección de datos personales en los países de la Unión Europea", *Revista Jurídica de Castilla y León*, Nro. 16 (2008):113-168.

titular de los datos la capacidad de ejercer –con certeza y coherencia– el control sobre el uso y la finalidad de dichos datos.

Precisamente, la promulgación de la LOPD en mayo de 2021 está llamada a desarrollar estos presupuestos, por cuanto en su exposición de motivos se invoca la imperiosa necesidad de generar confianza y garantizar las oportunidades que brindan los adelantos tecnológicos[12]. Naturalmente, como señalan dichas motivaciones, por una parte, todo esto "obliga a los países a realizar marcos jurídicos compatibles en distintos niveles: nacional, regional y mundial que faciliten el intercambio y al mismo tiempo respeten y protejan los derechos humanos"; y, por otra, se espera que su normativa "salvaguarde los derechos, promueva la actividad económica, comercial, de innovación tecnológica, social, cultural, entre otras y delimite los parámetros para un tratamiento adecuado en el ámbito público y privado".

Además, por mandato constitucional, es preciso destacar que la LOPD de Ecuador es el resultado de un proceso legislativo que trata de fortalecer la integración en Latinoamérica y el Caribe, toda vez que el Estado ecuatoriano está comprometido en "fortalecer la armonización de las legislaciones nacionales con énfasis en los derechos (..), de acuerdo con los principios de progresividad y no regresividad" –art. 423.3–. En todo caso, tanto de la exposición de motivos como de los considerandos, observamos que la nueva normativa de protección de datos personales resalta la trascendencia en el ámbito internacional del Reglamento (UE) 2016/679; de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, en 2017; y de los Principios de Privacidad y Protección de Datos Personales de la OEA, en 2015. Esto nos lleva a pensar que la LOPD, no solamente está orientada

[12] La Ley Orgánica de Protección de Datos Personales fue publicada en el Registro Oficial, Quinto Suplemento, Nro. 459, el 26 de mayo de 2021. Fue aprobada por unanimidad con 118 votos afirmativos y una abstención –de un total de 119 asambleístas presentes–, durante la sesión 707 (en modalidad virtual) del pleno legislativo. Según la Segunda Disposición Transitoria, "todo tratamiento realizado previo a la entrada en vigencia de la presente Ley deberá adecuarse a lo previsto en la presente norma, dentro del plazo de dos años contados, a partir de su publicación en el Registro Oficial. El incumplimiento de la presente disposición dará lugar a la aplicación del régimen sancionatorio establecido en esta Ley".

a fortalecer una integración regional sino también a concretar un nivel adecuado de protección, basado en estándares globales[13].

Bajo estas consideraciones, a la luz de la Ley general aprobada en mayo de 2021, este capítulo se enfocará en estudiar, tanto el proyecto de "Ley Orgánica de la protección de los derechos a la intimidad y privacidad sobre los datos personales", presentado en 2016, como el "Proyecto de Ley Orgánica de Protección de Datos Personales", formulado en 2019. Además, con el objeto de contrastar con la experiencia internacional, invocaremos el marco jurídico europeo, con especial referencia al Reglamento (UE) 2016/679 y a la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales[14].

El objetivo propuesto es comparar y consensuar el contenido de la normativa ecuatoriana con la experiencia que el modelo europeo, incluso latinoamericano, ha desarrollado en la materia. Precisamente, tomando en cuenta que, en el contexto latinoamericano, no existe una Ley Modelo sobre protección de datos personales, abordaremos el contenido de los "Doce Principios de Privacidad y Protección de Datos Personales" de 2015, contenidos en la Guía Legislativa para los Estados Miembros de la OEA, por cuanto tal como lo ha señalado este organismo, este instrumento internacional tiene por objeto orientar a los Estados Miembros en la elaboración y desarrollo de Leyes nacionales sobre protección de datos personales.

Además, considerando que la Red Iberoamericana de Protección de Datos (RIPD), concretó en 2017 la aprobación de los "Estándares de Protección de Datos

[13] Como se desprende de la exposición de motivos de la LOPD, "es indispensable dar certidumbre a usuarios, empresas, organizaciones y Estados, sobre todo en este momento en el cual la economía mundial se desplaza más hacia un espacio de información masiva, híper-conectada, en tiempo real, de flujo incesante proveniente de internet de las cosas, automatizada con algoritmos de inteligencia artificial cada vez más sofisticados y de la réplica incesante mediante tecnologías de registros distribuidos.

[14] Hay que advertir que, si bien a lo largo de este capítulo hemos realizado referencias a la Ley Orgánica 15/1999 de protección de datos de carácter personal, mientras este estudio se encontraba en su fase final se aprobó la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales. Por tanto, consideramos pertinente, además, incluir las referencias actualizadas a este último cuerpo legal.

Personales para los Estados Iberoamericanos"[15]; citaremos las disposiciones relativas a los principios; definiciones; ámbito de aplicación; derechos y obligaciones; ejercicio de los derechos ARCO; transferencias internacionales de datos personales; medidas proactivas; autoridades de control; reclamaciones y sanciones; y mecanismos de cooperación internacional.

De esta manera, pretendemos sugerir un modelo adecuado, armónico y equilibrado de regulación que garantice la vigencia del derecho a la protección de datos en Ecuador. Principalmente, en este capítulo centraremos nuestra atención en el análisis del objeto, ámbito de aplicación, definiciones y tratamiento de datos sensibles, como instituciones que se derivan de la normativa de protección de datos personales. Lógicamente, la doctrina y también la jurisprudencia de la CCE contribuirá en la búsqueda del equilibri*o* para la garantía de este derecho, por medio de una propuesta que desarrolle el denominado pacto social*,* y que permita, a partir de la seguridad jurídica, el respeto a todos los derechos y libertades básicas implicadas en los tratamientos de datos.

## 2. Estudio del objeto, ámbito de aplicación y definiciones contenidas en la Ley general en Ecuador

### 2.1 Objeto del marco general de protección de datos personales

El derecho a la protección de datos personales se reconoce en la Constitución de Ecuador, como un derecho de libertad, el cual se encuentra tutelado, mediante el *habeas data*. Considerándolo como un instituto de garantía de otras libertades, se orienta a materializar, no solamente la protección de la información personal y el aseguramiento de las condiciones mínimas para su efectivo desarrollo sino, además, un conjunto de derechos y libertades fundamentales que protejan a la persona en relación con el tratamiento de sus datos personales.

[15] Puede considerarse a este instrumento internacional como una Ley Modelo para los Estados Iberoamericanos.

. La CCE explica que la protección de datos “comporta el derecho de toda persona a ejercer control sobre la información personal que le concierne, frente a cualquier ente público o privado” y, por tanto, “tiene un carácter instrumental, supeditado a la protección de otros derechos constitucionales que se pueden ver afectados cuando se utilizan datos personales, como puede ser la intimidad, la honra, la integridad psicológica, etc.”[16].

En este sentido, advertimos que el objeto del marco general de protección de datos se fundamenta en garantizar que el tratamiento respete los derechos y libertades de las personas, y en suma el derecho a la protección de datos personales. En todo caso, recordemos que este derecho implica ejercer facultades, control y decisión sobre los propios datos personales, y que las intromisiones ilegítimas –como resultado del tratamiento de dicha información–, pueden afectar derechos relacionados con el libre desarrollo de la personalidad. Si bien la CCE insiste en el carácter instrumental de este derecho fundamental, subrayamos que el objeto de la Ley comprende, tanto la tutela de los derechos y libertades en relación con el tratamiento como la protección de los datos personales que le pertenecen a las personas físicas.

En el caso de Ecuador, el proyecto de “Ley Orgánica de la protección de los derechos a la intimidad y privacidad sobre los datos personales” –en adelante PLODP 2016– planteaba que el objeto era proteger y garantizar “el derecho de todas las personas a la intimidad y privacidad en el tratamiento de datos personales que se encuentren en bases o bancos de datos, ficheros, archivos, en forma física o digital, en instancias públicas o privadas” –art. 1–. En primera instancia, parecía restringirse su objeto, por cuanto se hacía, únicamente, referencia a la protección de los derechos a la “intimidad y privacidad” sobre los datos personales. Así, corresponde señalar que el objeto de la normativa de protección de datos supone, no solamente proteger la información personal, a través de la intimidad y/o privacidad sino también comprende la tutela de otros bienes jurídicos, como el

[16] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC **–**CASO Nro. 67-11-JD**–** publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.

desarrollo de la personalidad, la integridad psicológica y, en suma, la dignidad de las personas. Por tanto, bajo este supuesto, "se intenta huir de considerar este derecho como un derecho absoluto para, en cambio, considerarse siempre en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad"[17].

Así también llamaba la atención que en el objeto del PLODP 2016, no exista referencia a la tutela del derecho a la protección de datos, por cuanto como hemos advertido en otro momento, "la protección de datos, siendo como es un derecho fundamental (…) impide (debería impedir) que la información disponible sobre las personas pueda ser utilizada en contra de sus derechos y libertades"[18]. Así, "se antoja necesario destacar a este respecto la postura que ha venido sosteniendo la jurisprudencia europea en cuanto a la ponderación que ha de existir siempre entre el derecho a la protección de los datos personales respecto de otros derechos en juego en cada caso concreto"[19]. Por tanto, el reconocimiento de la protección de este derecho es esencial, toda vez, que materializaría su desarrollo, a través de la Ley, y garantizaría confianza y seguridad jurídica en una norma destinada a proteger los datos, cuando este derecho entre en conflicto con otras libertades. De ahí que, sería inconstitucional limitar, únicamente, a estos derechos el desarrollo del derecho a la protección de datos, más aún, si el objeto de una Ley por el estilo, en una sociedad globalizada, pretende sumarse a un marco común y normas conexas para la garantía del derecho a la autodeterminación informativa en los Estados miembros de la OEA[20].

---

[17] Joaquín Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 336.

[18] Pablo Lucas Murillo de la Cueva y José Luis Piñar Mañas, El *derecho a la autodeterminación informativa* (Madrid-México: Fontamara S.A, 2011), 109.

[19] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 336.

[20] La Guía legislativa de la OEA, adoptada en el 86 período ordinario de sesiones del Comité Jurídico Interamericano en 2015, sobre el concepto de privacidad anota que: "la constitución y las Leyes fundamentales de muchos Estados Miembros de la OEA garantizan el respeto y la protección de la privacidad, la dignidad personal y el honor familiar, la inviolabilidad del hogar y las comunicaciones privadas, los datos personales y conceptos conexos. Casi todos los Estados Miembros de la OEA han adoptado algún tipo de Ley con respecto a la protección de la privacidad y los datos (aunque

Además, llamaba la atención que el PLODP 2016 señale en su objeto cuestiones relativas al ámbito de aplicación. Por ejemplo, esta propuesta determinaba que la Ley se destinaría a proteger "el tratamiento de datos personales que se encuentren en bases o bancos de datos, ficheros, archivos, en forma física o digital, en instancias públicas o privadas" –art. 1–. Como sabemos, uno de los supuestos para que opere la seguridad jurídica es la existencia de normas jurídicas claras. Por ello, no debía confundirse en su objeto preceptos relacionados con el ámbito de aplicación.

En todo caso, el proyecto de "Ley Orgánica de Protección de Datos Personales" –en adelante PLODP 2019– precisó que el objeto de esta Ley se enmarcaba en "regular el ejercicio del derecho a la protección de datos, la autodeterminación informativa, y demás derechos digitales en el tratamiento y flujo de datos personales, a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela" –art. 1–. Puede decirse que esta propuesta, era muy completa y se adecuaba a las exigencias que plantea el derecho a la protección de datos personales. Incluso, al igual que la normativa internacional, su objeto estaba orientado a garantizar el flujo o la libre circulación de datos. No obstante, la LOPD ha establecido que su objeto es "garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela" –art. 1–. Con ello, por una parte, el legislador ha olvidado reconocer la protección de otros derechos y libertades, que pueden estar relacionados con este derecho fundamental; y, por otra, además, no ha estatuido en su objeto una regulación expresa sobre la libre circulación de los datos personales.

sus disposiciones varían considerablemente en lo que se refiere a su enfoque, ámbito de aplicación y contenido)". En todo caso, conviene señalar que, según el art. 77 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, cualquier persona puede ejercer una demanda de inconstitucionalidad y, así ejercer el derecho al control abstracto de constitucionalidad, el cual tiene por finalidad "garantizar la unidad y coherencia del ordenamiento jurídico a través de la identificación y la eliminación de las incompatibilidades normativas, por razones de fondo o de forma, entre las normas constitucionales y las demás disposiciones que integran el sistema jurídico" –art. 74–.

Desde la perspectiva comparada, el Reglamento (UE) 2016/679 –en adelante RGPD– precisa en su objeto que "establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos" –art. 1.1–; y la protección de "los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales" –art. 1.2–. De esta manera, el objeto del RGPD se enmarca en "fijar los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal sin atender a su nacionalidad o residencia y respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal"[21].

En el mismo sentido, la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales –en adelante LOPDGDD–, encargada de adaptar el ordenamiento jurídico español al RGPD y completar sus disposiciones, precisa en su objeto tutelar "el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución" –art. 1.a)–; y, además, garantizar "los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución"–art. 1.b)–[22].

[21] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 335.

[22] La derogada Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de España –en adelante LOPD– estimaba en su objeto "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar" –art. 1–. Ahora bien, sobre la inclusión en el objeto de la LOPDGDD de la garantía de nuevos derechos digitales, entendemos que "las categorías tradicionales sobre las que se asienta el derecho a la protección de datos han evidenciado su debilidad y exigen una adecuación a los tiempos actuales que constituyen uno de los principales retos del REPD al actualizar su aplicación al nuevo entorno tecnológico y al crear nuevos derechos digitales". Cfr. Artemi Rallo Lombarte, "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)", UNED: Revista de Derecho Político, Nro. 100 (2017), 639-669. En todo caso, esta adecuación "trae como consecuencia que el ámbito de aplicación de la LOPDGDD, recogido en su art. 2, se aparte del ámbito de aplicación material del art. 2 RGPD que se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Se genera un cierto desorden en el ámbito de aplicación de la LOPDGDD que se evidencia con una simple lectura de su art. 2. Esto es así porque muchos de los llamados derechos digitales –al menos expresamente los regulados en los arts. 79 al 88 y 95 al 97– no son derechos de protección de datos personales y no protegen a las personas físicas en relación con el tratamiento de sus datos

A diferencia de los textos jurídicos comparados que se anotan, el objeto del PLODP 2016 suponía, una vez más, la única protección de los derechos de intimidad y privacidad. Sin embargo, tanto el RGPD como la LOPDGDD coindicen en que –en lo que respecta al tratamiento de los datos personales–, el objeto es la protección y la tutela de las libertades y derechos fundamentales, en particular del derecho a la protección de datos personales. Es evidente que el PLODP 2016 debía contemplar que la protección de datos personales, no solamente se haga, a partir de la intimidad y privacidad sino también con relación a los derechos y libertades que se ven afectados por el tratamiento de la información personal[23].

Ahora bien, como queda anotado, el PLODP 2019 estableció un objeto de protección más completo e idóneo, garantizando –al igual que el caso de España–, no solamente el derecho a la protección de datos personales sino también los derechos digitales. Además, reconocía la necesidad de garantizar las normas relativas a la libre circulación de la información de carácter personal[24]. Naturalmente, a condición de que la normativa aprobada en la LOPD pueda completarse, mediante su reglamento, advertimos que, "el objeto, por tanto, es doble: regular un derecho (la protección de datos) y garantizar una libertad (la libre circulación de los datos. No podemos pues ignorar esta realidad ni dejar de resaltarla"[25].

personales". Cfr. Antonio Troncoso, "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de Derechos Digitales", Derecom, Nro. 26 (2019): 131-140.

[23] Como señalan los Estándares de protección de datos personales para los Estados Iberoamericanos, la protección de este derecho fundamental "es compatible con el objetivo de garantizar y proteger otros derechos, los cuales se reconocen como indivisibles e interdependientes unos con otros".

[24] Si bien el art. 1 de la LOPD omite señalar este aspecto, advertimos que el Capítulo lX de dicha Ley se dedica a regular la transferencia o comunicación internacional de datos personales, señalando que ésta "será posible si se sujeta a lo previsto en el presente capítulo, la presente Ley o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales" –art. 55–.

[25] José Luis Piñar Mañas, "Objeto del Reglamento", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 52.

### 2.2 Ámbito de aplicación

El PLODP 2016 precisaba que los principios y disposiciones contenidas en esta Ley se aplicarían a los datos personales "registrados en cualquier base de datos que los haga susceptibles de tratamientos por entidades de naturaleza pública o privada, en todo el territorio nacional" –art. 2–. Así, del texto propuesto, aunque repetitivo con la norma que refería al objeto de la Ley, se destacaba la regulación integral del tratamiento de la información personal, en sede tanto pública como privada[26].

Ahora bien, el PLOPD 2019 distinguió un ámbito de aplicación, tanto material como territorial. En lo material, se advirtió que se aplicaría al tratamiento de datos personales "contenidos en cualquier tipo de soporte, ya sean totalmente automatizados, parcialmente automatizados o no automatizados" –art. 3–. Además, en lo territorial –sin perjuicio de la normativa adoptada en instrumentos internacionales–, se señalaba que se aplicaría a tratamientos realizados en cualquier parte del territorio y también para los tratamientos fuera del territorio nacional –art. 4–. Sobre este respecto, apuntamos que, a diferencia del PLOPD 2019, la LOPD ha agregado en el ámbito de aplicación material que se aplicará sobre "cualquier tipo de soporte, automatizado o no, *así como a toda modalidad de uso posterior*" –art. 2–. En todo caso, con relación al ámbito territorial, se mantiene el texto señalado en el PLOPD 2019, de conformidad a lo establecido en el art. 3 de la LOPD.

La LOPD recoge un idéntico marco de aplicación establecido en el RGPD, por cuanto éste distingue también un ámbito de aplicación material y territorial. Así, en el ámbito material determina que "se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero" –art. 2.1–; y en el ámbito territorial, "se aplica al tratamiento de datos personales en el contexto

[26] Según la Guía legislativa de la OEA, orientada a preparar e implementar Leyes nacionales y normas conexas en los Estados Miembros, el ámbito de aplicación es aplicable al ámbito público y privado, "es decir, tanto a los datos personales generados, recopilados o administrados por entidades públicas como a los datos recopilados y procesados por entidades privadas. Se aplican tanto a los datos personales impresos como a los archivos electrónicos".

de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no" –art. 3.1–. En este marco, entendemos que el ámbito de aplicación material dispuesto en el RGPD "especifica que la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas, por lo que no se hará distinción entre los tratamientos automatizados o no automatizados de datos personales"[27]; y en el ámbito de aplicación territorial, supone el cumplimiento de la normativa para responsables y encargados del tratamiento "con establecimiento en la Unión Europea, independientemente de donde tenga lugar dicho tratamiento, y amplía este ámbito de aplicación territorial incluyendo también a responsables o encargados que, aun no estando establecidos en la Unión Europea, ofrecen bienes o servicios a interesados en la Unión Europea"[28].

Por otra parte, el ámbito de aplicación de la LOPDGDD está dirigido a regular "cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero" –art. 2.1–[29]. En este contexto, destacamos que:

> Teniendo en cuenta la regulación del ámbito de aplicación material –art. 2.1 RGPD y art. 2.1 LOPDGDD–, podemos distinguir la existencia de dos tipos de tratamientos de datos personales: los tratamientos automatizados de datos personales –que lo pueden ser total o parcialmente– y los tratamientos no automatizados. Afirmar la existencia de un tratamiento automatizado no ha supuesto hasta ahora ningún problema: hay tratamiento automatizado cuando se aplica la informática o las tecnologías de la información y la comunicación[30].

De las normas expuestas, el ámbito de aplicación material del marco normativo de protección de datos está orientado a regular el tratamiento automatizado y no automatizado. A pesar de que el PLOPD 2016 proponía que la protección de los datos –contenidos en soporte físico o electrónico–, se garantice en el objeto de la

[27] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 337.

[28] Ibíd., 339.

[29] La LOPD 15/1999 estimaba en su ámbito de aplicación regular "los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado".

[30] Antonio Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada*, Nro. 49 (2018), 187-266.

Ley, advertimos que este reconocimiento debía hacerse en su ámbito de aplicación, tal como lo propuso el PLOPD 2019, que ahora es Ley en nuestro país. En este orden, es adecuado considerar que el ámbito de aplicación para la protección de los datos personales debe corresponder a una tutela integral y ordenada de la información, ya sea por medios convencionales o manuales y electrónicos[31], teniendo en cuenta, "la evolución y multiplicación de los medios de comunicación y de difusión de información"[32], toda vez que el acopio de la información y su tratamiento por cualquier medio representa un riesgo para los bienes jurídicos, que garantiza este derecho fundamental.

Conviene señalar que –al igual que el RGPD–, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos –en adelante EPEI– distinguen un ámbito de aplicación material u objetivo y territorial[33], pero además, precisa un marco de aplicación de carácter subjetivo, el cual es aplicable "a las personas físicas o jurídicas de carácter privado, autoridades y organismos públicos, que traten datos personales en el ejercicio de sus actividades y funciones" –art. 3.1–[34]. Como ha señalado la CCE, en este caso el ejercicio del derecho fundamental a la protección de datos no se limita a la calidad de las personas jurídicas; sin embargo, este derecho, únicamente, "puede extenderse a sus socios, representantes legales y

[31] Sobre esta parte, la CCE expone que: "no interesa para el *habeas data*, como garantía, el papel y la tinta utilizados para registrar el dato, ni el disco duro en el cual se encuentre la información –denominados por el constituyente como "soporte material o electrónico" de los datos–, ni cualquier forma ideada por el ingenio humano para su preservación, sino que, como la expresión lo señala, el derecho tutelado recae sobre el dato mismo y el uso informativo que se le dé". Cfr. Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 67-11-JD– publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.

[32] Lucas Murillo de la Cueva y Piñar Mañas, El *derecho a la autodeterminación informativa*, 115.

[33] Respecto al ámbito de aplicación material u objetivo, los EPEI señalan que "serán aplicables al tratamiento de datos personales que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización" –art. 4.1–. Así también sobre el ámbito de aplicación territorial determinan que "serán aplicables al tratamiento de datos personales efectuado: Por un responsable o encargado establecido en territorio de los Estados Iberoamericanos" –art. 5.1. a)–.

[34] Corresponde aclarar que, el RGPD "no entra a regular el tratamiento de datos personales relativos a personas jurídicas y, en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto". Cfr. Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 337.

personas relacionadas, en tanto la posición que ocupan y la relación jurídica establecida respecto de la persona jurídica, y estrictamente respecto de ellas"[35].

Si bien el art. 2. g) de la LOPD, estima que la Ley, no será aplicable a "los datos que identifican o hacen identificable a personas jurídicas", advertimos que el PLOPD 2016 suponía proteger y garantizar el derecho a la protección de datos de las personas en general –art. 1–, es decir, tanto físicas o naturales, como jurídicas o morales, en calidad de titulares de este derecho fundamental. Esta constituyó una previsión novedosa ya que, como señalan los EPEI, por regla general, el marco de protección de datos es aplicable a las personas físicas[36], pero además, no se impide la aplicación de la legislación, en el caso de las personas jurídicas. Con referencia a este aspecto, recordemos que la CCE apunta que:

> El término 'personas' en tanto se refiere a la titularidad de los derechos constitucionales, no debe excluir a priori a una especie del género, como son las personas jurídicas (…) El derecho a la protección de datos personales tiene un contenido complejo y comporta diversas dimensiones relacionadas con la información "personal" (…) Dichas dimensiones del derecho pueden ser perfectamente cumplidas si son aplicadas a una persona jurídica, por lo que no se advierte razones para negar la titularidad del mismo ni, en consecuencia, limitar su acceso al *habeas data*, como mecanismo de tutela en sede de jurisdicción constitucional[37].

Por tanto, la CCE concluye que:

> Por las características del derecho a la protección de datos personales, no se considera constitucionalmente adecuada la limitación a la calidad de las personas jurídicas como titulares del mismo; sin embargo, la información personal de dichos sujetos únicamente se extiende a las personas asociadas o a sus representantes legales, en tanto a la calidad que ostentan respecto de la persona jurídica, con estricto respeto al derecho a la protección de los datos personales y derechos conexos que le son atinentes a su naturaleza[38].

Desde esta perspectiva, aclaramos que:

> La finalidad del tratamiento no delimita el ámbito de aplicación del derecho fundamental a la protección de datos personales, que tiene como ámbito objetivo de aplicación la existencia de datos personales sometidos a tratamiento. Cualquier dato personal, también los datos de

[35] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 67-11-JD– publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.
[36] Este instrumento señala que excepcionalmente la legislación "no impide que los Estados Iberoamericanos en su legislación nacional dispongan que la información de las personas jurídicas sea salvaguardada acorde con el derecho a la protección de datos personales" –art. 4.2–.
[37] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 67-11-JD– publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.
[38] Ibíd.

> puesto profesional y de vinculación con una empresa o de actividad comercial o industrial, sometidos a tratamiento puede implicar una vulneración de nuestros derechos fundamentales, permitiendo establecer perfiles o clasificaciones que impidan el ejercicio de los derechos y el libre desarrollo de la personalidad. No tendría sentido que este derecho fundamental protegiera los datos identificativos y de domicilio de una persona física y no protegiera al mismo tiempo los datos relativos al puesto profesional o a la actividad comercial o industrial[39].

Esta relevante aclaración resulta, más que necesaria, toda vez que surge de la necesidad de evidenciar posibles limitaciones en la tutela del derecho a la protección de datos personales. Ahora bien, en relación al ámbito de aplicación material u objetivo que señalan los EPEI, la normativa puede ser aplicable al tratamiento de datos personales "que obren en soportes físicos, automatizados total o parcialmente, o en ambos soportes" –art. 4.1–. Si bien, la CCE aclara que para la garantía de este derecho, a través del *habeas data,* no es importante el soporte material o electrónico en el que se encuentran los datos, por cuanto "el derecho tutelado recae sobre el dato mismo y el uso informativo que se le dé"; advertimos que, "más complejo ha sido la delimitación de la existencia de un tratamiento de datos personales no automatizado"[40], lo cual afecta a la información personal que se encuentra en soportes físicos o en papel. Por ello, entendemos que:

> A los efectos del RGPD, que existe un tratamiento no automatizado de datos personales –un tratamiento manual- cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él, existiendo fichero cuando hay un conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados (…) De esta forma, es de aplicación el derecho fundamental a la protección de datos personales –los derechos de las personas y las obligaciones de los responsables de tratamiento- cuando la información personal en papel procede o es producto de un fichero manual-estructurado en virtud de personas[41].
> .

Por otra parte, respecto al ámbito de aplicación territorial, los EPEI –al igual que el RGPD– establecen que la normativa de protección de datos tiene efectos en el ámbito nacional y supranacional –art. 5–. Precisamente, en este caso, consideramos que una de las virtudes del RGPD "es establecer un nivel de

[39] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 952-953.

[40] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 200.

[41] Ibíd., 201, 202.

protección «equivalente en todos los Estados miembros», y garantizar una aplicación de estas normas «coherente y homogénea». Existirá, por lo tanto, un único paneuropeo que reemplazará los derechos nacionales"[42]. Por ello, valga la oportunidad para insistir en la necesidad de un marco común, que en Latinoamérica asegure, no solamente confianza en el marco de protección de datos sino, además, facilite el desarrollo tecnológico y la economía digital. De esta forma, evidenciamos que conforme el PLOPD 2016, la normativa hubiese aplicado, únicamente, en territorio nacional –art. 2–[43]. En todo caso, la LOPD –bajo los términos que propuso el PLOPD 2019 en el art. 4.5– ha reconocido que se aplicará "al responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional, que le resulte aplicable la legislación nacional" –art. 3.4–.

Como es conocido, en el ámbito internacional un requisito que demuestra un nivel adecuado de protección de datos, es la regulación del flujo transfronterizo de la información personal. Así, tomando como ejemplo, la aplicación territorial del RGPD, la importancia radica en establecer "un campo de juego nivelado, que garantice tanto la libre circulación de los datos como la garantía homogénea del derecho de los ciudadanos a la protección de sus datos personales"[44]. A partir de la experiencia que demuestra Argentina y Uruguay dentro de la Comunidad Andina, la previsión de un marco jurídico, que en el ámbito extraterritorial permita la transferencia internacional de datos, y consecuentemente, proteja las libertades que se desprenden de este derecho; "sólo es posible si se consensuan unas normas de protección de datos personales -asumiendo que existen visiones diferentes en los distintos continentes- y si éstas se extienden a todos los países"[45]. En todo caso, como precisa la Guía Legislativa de la OEA, el principal objetivo que Latinoamérica debe plantearse es "armonizar los enfoques reguladores que proporcionan una

[42] Santiago Ripol Carulla, "Aplicación territorial del Reglamento", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 91.

[43] En todo caso, los arts. 20 y 21 de este proyecto establecían algunas excepciones, por las cuales podía efectuarse las transferencias internacionales de datos personales.

[44] Ripol Carulla, "Aplicación territorial del Reglamento", 92.

[45] Antonio Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, Nro. 43 (2012): 25-184.

protección más efectiva de la privacidad, al mismo tiempo que se promueven los flujos de datos seguros para el crecimiento económico y el desarrollo".

Finalmente, el PLODP 2016, en su ámbito de aplicación, reconocía las excepciones que se aplicarían sobre este marco de regulación. Las limitaciones correspondían "a la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros" –art. 2–. No obstante, el PLODP 2019 propuso tres excepciones relativas al ámbito de aplicación de la Ley, en cuanto a: "el tratamiento de datos personales utilizados en actividades familiares y domesticas" –art. 3.1–; datos anonimizados –art. 3.2–; y datos que identifican o hacen identificables a personas jurídicas –art. 3.3–. En todo caso, la LOPD ha cristalizado, además, que la Ley, no, será aplicable al tratamiento de datos personales sobre: personas fallecidas –art. 2. b)–; actividades periodísticas y otros contenidos editoriales –art. 2. d)–; materia de gestión de riesgos por desastres naturales y, seguridad y defensa del Estado –art. 2. e)–; y bases de datos para prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales –art. 2. f).

En este punto, corresponde señalar que el RGPD enumera como excepciones los tratamientos relacionados con: "el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión" –art. 2. a)– y, por tanto, el RGPD "únicamente es de aplicación a todas las actividades relacionadas con el tratamiento de datos personales en relación con actividades en las que la UE tenga competencias regulatorias"[46]. Así también el RGPD no se aplica al tratamiento de datos "por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE" –art. 2. b)–, es decir, "cuando realicen actividades de política exterior y de seguridad común (PESC), mientras que, si sería aplicable al resto de actividades que se realicen en

[46] Iñaki Uriarte Landa, "Ámbito de aplicación material", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 65.

desarrollo de la acción exterior de la unión"[47]. El RGPD, además, excluye la regulación de los tratamientos "efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas" –art. 2. c)–[48]. Como sucede con las excepciones que plantea la LOPD en el art. 2. a), esta exclusión significa que "los tratamientos que se realicen, en el marco de esta salvedad, no deben tener conexión alguna con una actividad profesional o comercial"[49]. Por ejemplo, se incluyen actividades relacionadas con la correspondencia; repertorio de direcciones y las acciones en redes sociales y en línea.

El RGPD, por último, establece como excepción los tratamientos "por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención" –art. 2. d)–. Así, cuando "los Estados encomienden a estas mismas autoridades funciones que no se lleven a cabo, necesariamente, con fines de persecución de infracciones penales, el tratamiento de datos personales para esos otros fines (…) les será de aplicación el Reglamento"[50]. Este es el supuesto de los tratamientos realizados por la Policía Nacional u otros organismos, "en unos casos realizan tratamientos con las finalidades de persecución de infracciones penales, pero, en otras ocasiones, realizan tratamientos que no están relacionados con estas finalidades, por ejemplo, los tratamientos de datos necesarios para la expedición del DNI"[51].

[47] Ibíd., 67.

[48] Sobre este respecto, el RGPD determina que "no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas" –Considerando 18–.

[49] Uriarte Landa, "Ámbito de aplicación material", 68

[50] Ibíd., 71.

[51] Ibíd.

Ahora bien, una novedad que introduce la LOPD es la excepción de los tratamientos de datos personales relacionados con datos anonimizados –art. 2. c)–. Al respecto, los EPEI establecen que la normativa de protección de datos no resulta aplicable, en el supuesto de la información anónima "es decir, aquélla que no guarda relación con una persona física identificada o identificable, así como los datos personales sometidos a un proceso de anonimización de tal forma que el titular no pueda ser identificado o reidentificado" –art. 4.3. b)–. En este orden, la LOPD hace bien al considerar que, "tan pronto los datos dejen de estar asociados o de ser anónimos, su tratamiento estará sujeto al cumplimiento de las obligaciones de esta Ley, especialmente la de contar con una base de licitud para continuar tratando los datos de manera no anonimizada o disociada" –art. 2. c)–.

Otro supuesto de exclusión es el tratamiento de datos de personas fallecidas. Por ejemplo, la LOPDGDD limita el ámbito de aplicación a "los tratamientos de datos de personas fallecidas, sin perjuicio de los establecido en el artículo 3" –art. 2.2. b)–[52]. Si bien, el RGPD no refiere en su ámbito de aplicación material excepciones relacionadas, sobre datos de personas fallecidas, en sus considerandos limita la aplicación de su normativa, frente a este supuesto[53]. No obstante, tanto el RGPD

[52] El art. 3 de la LOPDGDD señala que: "1. Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión (…) no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una Ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante. 2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión (…) 3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado".

[53] El RGPD establece que "no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas" –Considerando 27–. Frente a este mismo supuesto, los EPEI apuntan que "la legislación nacional de los Estados Iberoamericanos aplicable en la materia podrá reconocer que las personas físicas vinculadas a fallecidos o designados por éstos, ejerzan los derechos a que se refiere el presente estándar respecto a los datos personales de fallecidos que les conciernan" –art. 32.3–.

como los EPEI dejan a salvo el criterio de los Estados para establecer regulaciones vinculadas a los datos personales de fallecidos[54]. Sobre este respecto, subrayamos que, inicialmente, la LOPD exceptúa de su ámbito de aplicación el tratamiento de datos personales de personas fallecidas –art. 2. b)–, sin perjuicio de la regulación señalada en dicha Ley. Así, con un texto legal –idéntico a la LOPDGDD–, la LOPD reconoce que "los titulares de derechos sucesorios de las personas fallecidas, podrán dirigirse al responsable del tratamiento de datos personales con el objeto de solicitar el acceso, rectificación y actualización o eliminación de los datos personales del causante"; además, habilita su ejercicio a "las personas o instituciones que la o el fallecido haya designado expresamente para ello"; y, por último, en el caso del fallecimiento de menores y de personas con discapacidad, estas facultades "podrán ejercerse por quién hubiese sido su último representante legal" –art. 27–.

Bajo estas consideraciones, advertimos que existen dos elementos esenciales que posibilitan el aseguramiento del objeto y la delimitación del ámbito de aplicación material de la normativa de protección de datos, esto es "que exista un tratamiento y que este se sustancie sobre datos personales"[55]. Si bien la LOPD sigue la línea que plantea el RGPD, respecto al ámbito de aplicación de la normativa de protección de datos, "esta necesidad de homogenización y coherencia normativa viene motivada, como decimos, por una cierta sensación de riesgo e inseguridad jurídica que pueden tener los usuarios, particularmente evidente cuando se exponen al tratamiento de sus datos personales en el contexto de Internet"[56].

[54] Recordemos que el derecho a la protección de datos "no es sólo un derecho autónomo, sino que es una garantía institucional de otros derechos fundamentales. En ocasiones el derecho garantizado también se extingue con la muerte –cuando la protección de datos garantiza la propia libertad personal o la libertad sindical–; en otras, el derecho o los intereses jurídicos que le dan vida pueden no haberse extinguido, como es el caso de la intimidad personal. Hay que tener en cuenta que la protección de datos personales es especialmente un instituto de garantía del derecho a la intimidad". Cfr. Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 206.

[55] Ibíd., 198.

[56] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 336-337.

### 2.3 Principales definiciones

En relación a las definiciones relacionadas con el derecho a la protección de datos personales y el tratamiento de la información de carácter personal, este apartado pretende contextualizar la naturaleza de cada término, que supone la aplicación y regulación de este derecho fundamental. Para el correcto entendimiento y ejercicio de este derecho –dentro del Estado constitucional de derechos y justicia–; es esencial promover en la sociedad, especialmente, en los poderes públicos –sea en el ámbito administrativo o judicial–, el respeto y garantía de la seguridad jurídica, como base para la confianza ciudadana y coherencia del marco jurídico. Como precisa la CCE:

> Los jueces tienen el deber ineludible de respetar y hacer respetar el ordenamiento legal diseñado para cada procedimiento, con la finalidad de tutelar los derechos garantizados en la Constitución, dicho de otro modo, son los jueces los garantes llamados a proteger los derechos garantizados en la Constitución dentro de los lineamientos predeterminados. Por lo tanto, la sumisión al mandato de las Leyes permite que las decisiones se logren en estricto derecho, todo fallo responde a lo que el derecho ordena más no a valoraciones personales[57].

Recordemos que, si bien la CCE hace referencia al deber de las autoridades administrativas y judiciales de respetar y hacer respetar el ordenamiento jurídico, mediante, la sumisión a la Constitución y al mandato de las Leyes –art. 11.3–; esta obligación también incluye a los particulares[58]. Por ello, la justificación de aclarar la naturaleza de los distintos conceptos responde, en primer término, a la necesidad de garantizar la confianza en el ordenamiento jurídico, a través de normas claras que impidan valoraciones subjetivas o de índole personal. En todo caso, las definiciones aportarán a una interpretación coherente de la legislación sobre protección de datos, de tal modo que ayude y clarifique la aplicación homogénea del régimen jurídico, tanto en el ámbito nacional como supranacional[59]. Así, como determina el RGPD, para garantizar un marco uniforme y elevado se debe asegurar

[57] Véase la Resolución de la Corte Constitucional 287, Sentencia Nro. 287-16-SEP-CC –CASO Nro. 578-14-EP– publicada en el Registro Oficial Suplemento Nro. 854 de 4 de octubre de 2016.

[58] En este punto, la CCE advierte que "la aplicación y eficacia directa de la Constitución implica que los jueces y los demás operadores jurídicos, incluyendo los particulares, habrán de tomar a la Constitución como una regla de decisión". Véase el Registro Oficial Suplemento 451 de 22 de octubre del 2008. Corte Constitucional del Ecuador. (2008). Resolución S/N.

[59] María Arias Pou, "Definiciones a efectos del Reglamento General de Protección de Datos", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 117.

“que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea” –Considerando 10–.

Entendiendo que el ejercicio del derecho a la protección de datos personales conlleva el cumplimiento de una serie de deberes de quienes intervienen en el tratamiento de la información personal, subrayamos que estas obligaciones “que pesan sobre quienes pretendan tratar información personal, contrapartida de los derechos y de las exigencias de los principios, comportan, junto a su estricto respeto, la observancia de formas y procedimientos imprescindibles para hacer efectivas las garantías del derecho a la autodeterminación informativa[60]. Por estas razones, en virtud de la importancia de los distintos conceptos que se derivan de la normativa de protección de datos. A continuación, precisaremos algunas definiciones relacionadas con los ficheros, bases de datos, responsable del tratamiento, titular de los datos, etc. Atendiendo, tanto los proyectos de 2016 y 2019 como la LOPD aprobada en mayo de 2021, contrastaremos la normativa del RGPD y los EPEI, con el objeto de identificar aciertos y errores en la normativa de protección de datos de Ecuador.

### 2.3.1 Base o bancos de datos (ficheros)

El concepto de “base” o “banco de datos” corresponde a lo que se conoce como un “fichero de datos”. Se trata de un concepto que representa la organización, estructuración y tratamiento de la información de carácter personal, por medio, de cualquier modalidad de almacenamiento y gestión, en donde se “pide a los responsables del tratamiento que las medidas de seguridad que implementen lo hagan atendiendo a un grado más de profundidad y se implanten a nivel de procesos de tratamiento de información”[61].

[60] Lucas Murillo de la Cueva y Piñar Mañas, El *derecho a la autodeterminación informativa*, 27.
[61] Muñoz Ontier, “Disposiciones Generales (Arts. 1-5)”, 342.

Según el Diccionario de la RAE, el fichero es un "conjunto organizado de informaciones almacenadas en un soporte común", el cual puede hacerse informáticamente; y la base de datos constituye una "memoria informática en la que pueden integrarse datos dispuestos de modo que sean accesibles individualmente por medios electrónicos o de otra forma". Así, entendemos que, este momento de la recogida de datos y su posterior registro y organización "hace que se pase de un dato personal aislado a un fichero, es decir, a un tratamiento automatizado o manual de esa información. A partir de ese momento se habla no de un dato de carácter personal sino de un fichero[62].

En este contexto, "para la determinación de que estamos en presencia de un tratamiento no automatizado o de un tratamiento manual"[63]; es primordial, definir qué se entiende por fichero. El PLODP 2016 definía a la base o banco de datos –fichero– como un "conjunto organizado de datos personales que es objeto de tratamiento o procesamiento, digital o no, cualquiera sea la modalidad de su formación, almacenamiento, organización o acceso" –art. 4.1–. No obstante, más completa parecía la definición del PLODP 2019, al considerar que una base de datos es "un conjunto configurado, estructurado o no estructurado de datos, cualquiera que fuere la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento y acceso" –art. 5.2–[64]. En todo caso, la LOPD ha completado esta definición, precisando que es un conjunto estructurado de datos "cualquiera que fuera la forma (…) localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica" –art. 4–.

Ahora bien, tanto la Guía Legislativa de la OEA como los EPEI no refieren definiciones sobre la naturaleza de los ficheros, bases o banco de datos. Por ello, advertimos que la LOPD sigue la definición del RGPD, la cual conceptualiza al fichero como "todo conjunto estructurado de datos personales, accesibles con

[62] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 416-417.
[63] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 200.
[64] Con una definición bastante similar, la LOPD 15/1999 estimaba que un fichero es "todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso" –art. 3.b)–.

arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica" –art. 4.6–. De esta manera, un fichero constituye "un conjunto estructurado de datos personales cuando la documentación está organizada conforme a criterios específicos relativos a las personas que faciliten el acceso de forma sencilla a los datos"[65].

De las definiciones que se transcriben, destacamos que los ficheros pueden almacenarse y gestionarse por cualquier vía –automatizada o no–, en que se trate la información personal. Así también las garantías sobre el tratamiento de datos en ficheros automatizados, sean éstos de naturaleza pública o privada[66]. Si bien los PLODP de 2016 y 2019, coincidían con la normativa europea, en cuanto a la naturaleza de las bases de datos o ficheros, la LOPD ha completado y concretado, sobre la base de la definición de fichero que realiza el RGPD.

### 2.3.2 Consentimiento del titular (consentimiento del interesado)

El consentimiento constituye una garantía de legitimación de los tratamientos de la información personal. Significa un elemento de determinación de la legitimación o licitud de los tratamientos de datos personales. Como señalan los EPEI, el consentimiento es la "manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen*"* –art. 2.1. b)–. Por tanto, esta garantía "atribuye a la persona un conocimiento y, por tanto, facilita un control sobre sus datos personales sometidos a tratamiento, de manera que pueda, en su caso, prestar el consentimiento y ejercitar sus derechos"[67].

---

[65] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 202.

[66] Como señala el RGPD, "en los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema" –Considerando 67–.

[67] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 453.

Puede decirse que el consentimiento, se encuentra incardinado con ciertas manifestaciones de la voluntad que hacen que el tratamiento sea legítimo, únicamente, cuando ha sido aceptado y autorizado por el titular. Es decir, "realizar cualquier tipo de operación –ya sea recopilación, grabación, utilización, modificación, comunicación, acceso, transferencia, conservación o archivo– con datos personales de otros requiere, de entrada, estar autorizado para ello"[68]. De esta manera, uno de los elementos para que la manifestación de la voluntad sea válida es el respeto del concepto de autodeterminación en lo que refiere a la información –derecho de información– que advierte al titular, afectado o interesado sobre las finalidades, prácticas y políticas por las cuales se tratarán los datos personales. Sobre este respecto, la Guía Legislativa de la OEA apunta que "se debe informar a la persona sobre los fines en el momento en el cual se recopilen los datos y se debe obtener su consentimiento en ese momento"[69], lo cual, evidentemente, exige que "el consentimiento consista siempre en una acción afirmativa del usuario, suponiendo una manifestación de voluntad libre, específica, informada y, como novedad, también inequívoca"[70].

En este orden, el PLODP 2016 definía el consentimiento como "toda manifestación de voluntad, libre, inequívoca, especifica e informada, mediante la cual el titular autoriza el tratamiento de datos personales" –art. 4.2–. Asimismo, el PLODP 2019 señaló que es la "manifestación de voluntad libre, previa, específica, expresa, informada e inequívoca, por la que el titular de los datos personales autoriza al responsable del tratamiento de datos personales a tratar los mismos" –art. 5.3–[71]. En todo caso, a partir del PLODP 2019, LOPD ha eliminado la palabra "expresa", para guardar conformidad con las disposiciones con los EPEI –art. 4–. En principio,

[68] Ramon Oró, *La protección de datos*, (Barcelona: Oberta UOC, 2015), 62

[69] La definición que hace el Diccionario de la RAE, sobre el consentimiento informado en el ámbito médico encaja, perfectamente, en materia de tratamiento de datos personales, por cuanto se considera a aquel "que ha de prestar el enfermo o, de resultar imposible, sus allegados, antes de iniciarse un tratamiento médico o quirúrgico, tras la información que debe transmitirle el medico de las razones y riesgos de dicho tratamiento".

[70] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 343.

[71] Sobre esta definición, la LOPD 15/1999 señalaba que el consentimiento es "toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen" –art. 3.b)–.

nos parece que esta definición tiene correspondencia con el derecho constitucional reconocido en el art. 66.19, y a su vez, respeta lo previsto en el *habeas data,* en cuanto a garantizar que "la recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular" –art. 92–.

A diferencia del PLODP 2016 y la LOPD en Ecuador, tanto el art. 4.11 del RGPD como el art. 6.1 de la LOPDGDD, exigen en el consentimiento una clara acción afirmativa, definiendo, de esta manera, el consentimiento como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". Así, entendemos que "una de las principales novedades del RGPD reside no en el consentimiento como supuesto de legitimación del tratamiento sino en la forma de entender prestado ese consentimiento"[72]. Por tanto, "la novedad es que se especifican dos formas de expresar el consentimiento: a) mediante una declaración y b) mediante una acción"[73]. Con referencia a este punto, subrayamos que:

> El RGPD clarifica la regla del consentimiento como criterio de licitud de los tratamientos, regulándolo con mayor exigencia y rigor, para que, como hemos señalado antes, no se le llame consentimiento a lo que no lo es –por ejemplo, para que al interés legítimo no se le presente como un consentimiento tácito-, decantándose porque el consentimiento se produzca siempre por claras acciones afirmativas o declaraciones expresivas[74].

Como se evidencia, el PLODP de 2016 y 2019 eran, prácticamente, iguales. No obstante, para considerar que el consentimiento sea válido, el PLODP 2019 sí estableció la necesidad de que era primordial que "el responsable pueda demostrar que el titular manifestó su voluntad, a través de una declaración o acción clara, afirmativa o se deduzca de una acción del titular" –art. 14–. Se trata de un reconocimiento que ha sido desestimado por el legislador en la LOPD. Por tanto, la

[72] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 220.
[73] Borja Adsuara Varela, "El consentimiento", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 152.
[74] Ibíd.

normativa aprobada difiere con el RGPD y la LOPDGDD en la forma en la que se expresa la voluntad, sobre todo, cuando se refiere a que el consentimiento debe manifestarse, a través de una "clara acción afirmativa"[75]. En este sentido, enfatizamos en que una de las maneras en las que puede evidenciarse una acción afirmativa es, por ejemplo, cuando en una página web que utiliza *cookies* "se advirtiera en el comienzo de la navegación, de forma que, si el usuario sigue navegando en la web, estaría llevando a cabo la acción afirmativa"[76]. Bajo este supuesto, la acción afirmativa se orienta a identificar, en el titular de los datos personales, conductas conscientes e inequívocas de aceptación y voluntad para el tratamiento de la información. Por ello, el consentimiento debe darse:

> Mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, especifica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen. Puede ser una declaración por escrito, inclusive por medios electrónicos o una declaración verbal, si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta[77].

Con el objeto de precisar que el consentimiento ha sido entregado de modo inequívoco, era necesario que el PLODP de 2016 incorpore en su regulación que la manifestación de la voluntad se comprobaría, según acciones afirmativas claras[78]. Esto es, esencialmente, importante en entornos digitales ya que, como señala la Guía Legislativa de la OEA, el consentimiento "debe interpretarse de manera

---

[75] El RGPD sobre el consentimiento, a través de una clara acción afirmativa determina que: "debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en Internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta" –Considerando 32–.

[76] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 95.

[77] Arias Pou, "Definiciones a efectos del Reglamento General de Protección de Datos", 122.

[78] Como se verá más adelante, únicamente, el PLODP 2019, en el art. 14, hace referencia a que el titular de los datos personales debe expresar su voluntad a través de una declaración o acción clara, afirmativa, o se deduzca de una acción del titular.

razonable en el entorno tecnológico en rápida evolución en el cual se recopilan y usan datos personales en la actualidad". Por consiguiente, estos elementos son considerados como un tipo de regla que tiende a priorizar la garantía de la legitimidad de los métodos, para obtener el consentimiento del titular de los datos personales, a partir de la utilización de medios electrónicos[79].

Desde el principio de legitimidad del tratamiento de la información, e incluso, para que una determinada acción afirmativa sea lícita –dentro del concepto del consentimiento–, subyace el derecho a la información, toda vez, que "muchas veces la recogida de datos puede ser considerada desleal o ilícita por el incumplimiento del principio de información"[80]. Así, en el caso de ilegitimidad por falta de consentimiento y debida información, mediante medios electrónicos, la ilicitud en la recogida de datos "puede ser consecuencia de la utilización de procedimiento técnicos muy sofisticados –recogida de datos a través de cookies en Internet- o muy sencillos –cupones para un sorteo que no informan de la existencia de un fichero–"[81]. Por ende, carecerían de legalidad, por cuanto hace falta aquella manifestación de la voluntad, libre, inequívoca, especifica e informada que se materializa, por medio, del consentimiento.

En suma, las definiciones que realizaba el proyecto de 2019 se encontraba acorde a lo que la normativa internacional sugería. Sin embargo, a partir del concepto de consentimiento que ha concretado la LOPD –art. 4–, para asegurar que aquel sea obtenido por medios legítimos y, en suma, materializar la transparencia de los

[79] Bien puede citarse también las recomendaciones que se describen en la Guía Legislativa de la OEA sobre "Claridad y Consentimiento", en donde se establecen los métodos para obtener el consentimiento. En lo pertinente se señala que: "El método para obtener el consentimiento debe ser apropiado para la edad y la capacidad de la persona afectada (si se conocen) y para las circunstancias particulares del caso. No se requiere una forma específica de consentimiento, pero en principio debería reflejar la preferencia y la decisión fundamentada de la persona afectada. Evidentemente, el consentimiento obtenido bajo coacción o sobre la base de declaraciones falsas o incluso información incompleta o engañosa no puede cumplir las condiciones para la recopilación o el procesamiento legítimos (…) La índole del consentimiento podría variar según las circunstancias del caso. En los principios se reconoce que, en algunas circunstancias, el "conocimiento" podría ser la norma apropiada en los casos en que el procesamiento y la divulgación de datos satisfagan intereses legítimos. El consentimiento implícito podría ser apropiado cuando los datos personales en cuestión son menos sensibles y cuando se proporciona información razonable sobre el propósito y el método de recopilación de manera tal que se cumplan los requisitos de transparencia".
[80] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 419.
[81] Ibíd.

tratamientos, se reitera la importancia de que en su reglamentación existan previsiones adecuadas sobre las acciones afirmativas, las cuales deben ser claras y transparentes, ya que como señala la Guía Legislativa de la OEA “sin claridad, el consentimiento de la persona con respecto a la recopilación de los datos no puede ser válido”.

### 2.3.3 Datos de carácter personal

Los datos personales de una persona física “no son algo anecdótico sino que representan el registro de su vida, reflejan sus características, sus opciones vitales, debilidades”[82]. Ciertamente, el valor que significan los datos personales para el común de las personas puede ser, precisamente, algo “anecdótico”. No obstante, los tratamientos de la información –manuales y automatizados– dejan al descubierto que los datos personales representan una fuente de poder, y también medios para atentar sobre los derechos de las personas. A partir de los avances tecnológicos en las sociedades modernas, los datos personales han llegado a expresar verdaderas fuentes de poder cuando se usan para satisfacer intereses –económicos, políticos, religiosos etc.–, de terceras personas sin contar con el consentimiento del titular.

Por ello, uno de los elementos clave para la protección de la información es “el establecimiento de principios y deberes que legitimen el tratamiento de los datos personales, consistentes con la evolución social y tecnológica”[83].

> Los avances tecnológicos –en particular, el desarrollo de Internet– facilitan considerablemente el tratamiento y el intercambio de información, permiten compartir recursos tecnológicos, centralizar determinadas actividades y procesos, y abaratar costes en la prestación de servicios por las propias empresas, fuera del país en el que se encuentran establecidas. Estos avances permiten que los datos de naturaleza personal, siempre útiles

[82] Ibíd., 32.
[83] María Maqueo Ramírez, Jimena Moreno y Miguel Recio Gayo, “Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario”, *Revista de Derecho (Valdivia)*, Nro. 1 (2017), 95.

> e interesantes para el desarrollo de cualquier actividad a gran escala, puedan hoy circular internacionalmente de manera rápida y ser almacenados indefinidamente[84].

Los mecanismos utilizados para aprovechar, ilícitamente, los datos personales constituyen eventuales amenazas para los derechos y libertades, toda vez, que las intromisiones ilegítimas pueden llegar a afectar "seriamente a la forma en que ésta se desenvuelve normalmente en la sociedad, la manera en que es vista por sus familiares, por sus vecinos, por sus compañeros"[85]. Así, hay que recordar que el carácter instrumental que garantiza este derecho fundamental, no solamente protege el derecho a la intimidad de las personas, sino que, además, tutela aquellos ámbitos en los cuales una persona puede llegar a ser identificada e identificable.

Bajo estas consideraciones, los EPEI definen a los datos personales como "cualquier información concerniente a una persona física identificada o identificable"[86], los cuales, en suma, pueden expresarse en forma "numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo" –art. 2.1. c)–. Así también la Guía Legislativa de la OEA los conceptualiza como la información "que identifica o puede usarse de manera razonable para identificar a una persona en particular de forma directa o indirecta, especialmente por referencia a un número de identificación o a uno o más factores referidos específicamente a su identidad física, fisiológica, mental, económica, cultural o social"[87]. En este sentido, distinguimos una definición amplia, que incluye "toda aquella información que pudiera vincularse a una persona, tanto si esta información hace referencia a su identidad, a sus características o a su comportamiento, como si la información se utiliza para determinar o influir en la manera de tratar o evaluar a la persona"[88].

---

[84] Alfonso Ortega Giménez, "La desprotección internacional del titular del de derecho a la protección de datos de carácter personal", *Revista Castellano-Manchega de Ciencias Sociales*, Nro. 19 (2015), 37-56.

[85] Maqueo Ramírez, Moreno y Recio Gayo, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", 95.

[86] Los EPEI determinan que una persona es identificable "cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas" –art. 2.1 c)–.

[87] Sobre este respecto, la Guía Legislativa de la OEA agrega que "la palabra datos se usa intencionalmente en un sentido amplio a fin de conferir la protección más amplia posible a los derechos de las personas afectadas, independientemente de la forma particular en que se recopilen, se almacenen, se recuperen, se usen o se difundan los datos".

[88] Ramon Oró, *La protección de datos*, 52.

Ahora bien, el PLODP 2016 estimaba que los datos personales significaban "cualquier información vinculada o que pueda asociarse a una o varias personas naturales identificadas o identificables", entre los cuales se encontraban: "nombres y apellidos, fecha de nacimiento, dirección domiciliaria, correo electrónico, número de teléfono, número de cedula, matricula vehicular, información patrimonial e información académica o cualquier otra información vinculada con la identidad del titular" –art. 4.3–. Asimismo, el PLODP 2019 estableció que la información personal era un "dato que identifica o hace identificable a una persona natural directa o indirectamente, en el presente o futuro. Los datos inocuos, metadatos o fragmentos de datos que identifiquen o hagan identificable a un ser humano, forman parte de este concepto"[89] –art. 5.6–. Si bien estos proyectos proponían una amplitud sobre lo que podía constituir un dato personal, bastaba con el texto inicial en el cual se atribuya la calidad de datos personales a aquella información sobre una persona física identificada o identificable. Precisamente, la LOPD ha considerado este aspecto al reconocer que los datos personales son aquellos que "identifica o hace identificable a una persona natural directa o indirectamente" –art. 4–.

Por otra parte, destacamos el criterio que ha precisado la CCE en cuanto a la diferencia existente entre dato e información. Así, la Corte precisa que:

> Los datos y la información serían conceptos asimilables, en tanto un dato sería la especie de información apta para ser procesada de diversas formas. Sin embargo, se ha identificado en la doctrina sobre la protección de datos una distinción entre los conceptos "dato" e "información" (…) De acuerdo con la distinción conceptual citada, el dato adquiere la calidad de información en tanto cumple una función en el proceso comunicativo. La información, entonces, requiere una interpretación del dato, que dota de carga valorativa y funcionalidad concreta a la descripción que éste hace. Por lo tanto, el dato solamente es relevante para la protección por medio del *habeas data*, en la medida en que sea susceptible de cumplir una función informativa (…) Como conclusión, los datos están protegidos por medio de la garantía constitucional del *habeas data*, siempre que cumplan con una función informativa respecto de las personas y sus bienes y, por ende, su comunicación, interpretación o tratamiento afecta en mayor o menor medida los derechos de aquel a quien se refieren[90].

Los datos personales se encuentran protegidos, además, por la garantía del *habeas data,* cuando cumplen una función informativa y que, en todo caso, puedan

[89] La definición propuesta en el PLOPD 2019 tiene particular relación con los términos bajo los cuales también se definen a los "datos personales" en la Guía Legislativa de la OEA.

[90] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 67-11-JD– publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.

identificar o hacer identificable a una persona[91]. Por tanto, como señala la Corte, debe garantizarse el control y dominio en su tratamiento, ya que "el objeto de la protección de datos es proporcionar a su titular mecanismos de defensa adecuados y efectivos frente a la obtención o tratamiento ilícito de la información de naturaleza personal"[92]. En efecto, este derecho fundamental –que incluye el acceso y la decisión sobre información y datos de este carácter– es garantizado, mediante, la vía jurisdiccional por el *habeas data,* que permite ejercer el conocimiento y acceso a los datos personales que consten en entidades públicas o privadas.

En este orden, el RGPD define como datos personales "toda información sobre una persona física identificada o identificable" –art. 4.1–*.* Al igual que los EPEI, el RGPD establece que "se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador" –art. 4.1–[93]. De esta manera, el RGPD introduce nuevas referencias sobre datos personales traducidas en "nuevas formas desarrolladas por la tecnología que nos permiten llegar a identificar a una persona y que están muy

[91] Respecto a la distinción entre dato e información personal que realiza la CCE, la Guía Legislativa de la OEA expone que: "en general, en los principios se evita el uso de la frase "información personal", la cual, por sí sola, podría interpretarse en el sentido de que no incluye "datos" específicos tales como elementos fácticos, "*bits*" almacenados electrónicamente o registros digitales. Análogamente, la palabra "datos" podría interpretarse en el sentido de que no incluye compilaciones de hechos que, tomados en conjunto, permitan sacar conclusiones sobre la persona o las personas en particular. Por ejemplo, los detalles relativos a la estatura, el peso, el color del cabello y la fecha de nacimiento de dos personas podrían constituir "datos" que, al compararlos, revelen la "información" de que son hermano y hermana o tal vez gemelos idénticos. A fin de promover la mayor protección posible de la privacidad, estos principios se aplicarían en ambos casos y no permitirían que un controlador de datos efectuara distinciones de ese tipo".

[92] Ortega Giménez, "La desprotección internacional del titular del de derecho a la protección de datos de carácter personal", 38.

[93] Como ejemplos, el RGPD señala: "un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona" –art. 4.1–. De esta manera, "se mantiene el régimen preexistente en cuanto a que se considera dato personal cualquier información relativa a una persona física que, bien la identifique directamente, bien la pueda llegar a identificar poniendo en relación los datos que se tienen sobre ella y siempre que ello no suponga un esfuerzo desproporcionado en cuanto a los medios o el tiempo que se ha de emplear para llegar a identificarle". Cfr. Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 340.

relacionadas con desarrollos de aplicaciones móviles o con el desarrollo del Internet de las Cosas"[94].

Siguiendo el esquema de los instrumentos internacionales que quedan anotados, destacamos que la LOPD ratifica que un dato personal constituye aquel referido, tanto a una persona física identificada como identificable[95]. Tomando en cuenta que la importancia de la definición del concepto "datos personales" se encuentra en determinar qué tipo de información puede identificar o hacer identificable a una persona, también es fundamental diferenciar el significado de que una persona no sea identificada, pero sí identificable, sin esfuerzos desproporcionados, teniendo en cuenta el coste, el tiempo y la tecnología. En este punto, entendemos que:

> Es importante diferenciar el dato anónimo del dato de una persona no identificada pero sí potencialmente identificable. Especialmente en el ámbito de la atención sanitaria y de la investigación es muy importante precisar cuándo una persona física resulta identificable. Los criterios objetivos establecidos en el RGPD para dilucidar si estamos ante un dato anónimo o ante un dato personal –al ser la persona identificable, por existir una probabilidad razonable de identificación- son los medios que pueden ser utilizados para identificar a la persona –si supone una actividad desproporcionada o no-, especialmente los costes y el tiempo necesario para la identificación, teniendo en cuenta la tecnología disponible en ese momento. Esto significa que un dato inicialmente anónimo, con la evolución de la tecnología, puede convertirse en un dato de una persona identificable[96].

Conforme a lo anotado, apreciamos que la LOPD responde al contexto internacional para el marco de regulación de los datos personales, por cuanto hacen referencia a que éstos consisten en toda aquella información, que pueda identificar o hacer identificable de manera razonable a una persona.

### 2.3.4 Datos sensibles (especialmente protegidos)

Ciertos datos personales tienen la calidad de información sensible o especialmente protegida, por cuanto su conocimiento, divulgación y tratamiento por terceros

[94] Arias Pou, "Definiciones a efectos del Reglamento General de Protección de Datos", 118.

[95] Así también las propuestas de Ecuador se asemejan al texto de la LOPD 15/1999, que sobre los datos de carácter personal consideraba a "cualquier información concerniente a personas físicas identificadas o identificables" –art. 3.a)–.

[96] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 208.

pueden afectar o lesionar, en mayor medida derechos vinculados con la intimidad, dignidad y honor de las personas. Debido a los avances tecnológicos y el desarrollo de los procesos de integración comercial, este marco "redunda en un incremento de relaciones en las que está implicada la transferencia internacional de información sensible, con el consiguiente aumento de la litigiosidad y la creciente dimensión económica que está cobrando el libre tránsito de la información"[97].

Por ello, distinguimos que:

> Si bien, este derecho fundamental protege todo tipo de datos, sean o no íntimos, sean o no públicos, no supone el mismo nivel de injerencia en el derecho fundamental el acceso a un datos que es público y que no pertenece a la intimidad de una persona que el acceso a un dato que es propio del círculo íntimo de una persona o que afecta a su libertad ideológica o religiosa[98].

En este orden de cosas, los EPEI definen que los datos personales sensibles son "aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste" –art. 2.1. d)–[99]. Así también la Guía Legislativa de la OEA concreta que este tipo de información, "abarca los datos que afectan a los aspectos más íntimos de las personas"[100]. De este modo, los datos sensibles comprenden aquellas categorías o aspectos "más privados de la personalidad, como por ejemplo las relativas a su origen racial o étnico, a las opiniones políticas, a las convicciones religiosas o filosóficas, a la salud y a la sexualidad"[101].

---

[97] Ortega Giménez, "La desprotección internacional del titular del de derecho a la protección de datos de carácter personal", 39.

[98] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 781.

[99] De manera enunciativa, los EPEI distinguen como datos personales sensibles aquello que "puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física".

[100] Por ejemplo, la Guía Legislativa de la OEA describe que, dependiendo el contexto cultural, social o político, esta categoría de datos podría abarcar "datos relacionados con la salud personal, las preferencias sexuales, las creencias religiosas o el origen racial o étnico. En ciertas circunstancias podría considerarse que estos datos merecen protección especial porque, si se manejan o divulgan de manera indebida, podrían conducir a graves perjuicios para la persona o a discriminación ilegítima o arbitraria".

[101] Ramon Oró, *La protección de datos*, 54-55.

En el caso de Ecuador, el *habeas data* garantiza que, en el tratamiento de los datos sensibles, "cuyo archivo deberá estar autorizado por la Ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias" –art. 92–. Por tanto, se acredita que esta categoría de datos merece un régimen especial de protección que –con el objeto de asegurar la legitimidad en su tratamiento– exige adoptar garantías apropiadas, que materialicen la tutela efectiva del derecho a la protección de datos personales. Por consiguiente, el concepto de datos sensibles describe una tipología o categoría de datos personales que requieren "una protección reforzada en relación con otros datos que, aun siendo también personales, no afectan al núcleo esencial de la persona y a su esfera privada"[102].

Aclarada la naturaleza de esta tipología de datos, siguiendo los proyectos que se proponían en Ecuador, queda por aclarar cuál era la definición de datos sensibles o especialmente protegidos. Recordando que la Guía Legislativa de la OEA entiende que, la descripción de los tipos específicos de datos sensibles o especialmente protegidos deben establecerse en cada legislación o normativa nacional, atendiendo su entorno cultural y jurídico[103]; el PLODP 2016 definía que los datos sensibles hacían referencia a las características físicas de una persona, las cuales revelaban "el origen racial y étnico, las convicciones ideológicas, filosóficas o morales, las opiniones políticas, creencias religiosas, los datos genéticos, la información referente a la salud y a la vida sexual o cualquier otro dato vinculado con la intimidad del titular" –art. 4.4–. Así también el PLODP 2019 distinguió como datos sensibles los relativos a la: "etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento

[102] Ana Isabel Herrán, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, (Madrid: Dykinson, 2002), 210.

[103] Sobre esta parte, la Guía Legislativa de la OEA señala que: "En los Estados Miembros de la OEA hay una gran variedad de entornos culturales y jurídicos, razón por la cual es difícil decir de manera general qué tipos específicos de datos es categóricamente más probable que conduzcan a atentados particularmente graves contra los derechos e intereses de las personas. Por consiguiente, deben establecerse garantías apropiadas en el contexto de la legislación y la normativa nacionales, que reflejen las circunstancias imperantes en la jurisdicción pertinente, a fin de proteger en medida suficiente los intereses de las personas en materia de privacidad. Los Estados Miembros deben indicar claramente las categorías de datos personales que se consideren especialmente "sensibles" y que, por consiguiente, requieran una mayor protección".

indebido pueda dar origen a discriminación". En suma, todos aquellos, cuyo tratamiento "atenten o puedan atentar contra los derechos humanos o la dignidad e integridad de las personas" –art. 5.9–. Sin perjuicio del contenido de la propuesta de 2019, esta última parte ha sido modificada por la LOPD al determinar que, dentro de esta categoría de datos se incluyen aquellos cuyo tratamiento "atenten o puedan atentar contra los derechos y libertades fundamentales" –art. 4–.

Con referencia a este aspecto, subrayamos que la introducción de estos tipos específicos de datos proviene del mandato constitucional previsto en el art. 11.2, por el cual se reconoce la igualdad y la prohibición de discriminación. Así:

> La Constitución recoge todos los elementos reconocidos a nivel internacional para distinguir el trato igualitario del discriminatorio: enumera los criterios por los que se pueden discriminar y los prohíbe expresamente, en tanto la finalidad o consecuencia del trato distinto, menoscabe o anule el reconocimiento, goce o ejercicio de los derechos. Entre las categorías prohibidas, también encontramos novedades (…) se ha incluido el género, la cultura, ideología, el portar VIH, la diferencia física, el pasado judicial y la condición migratoria; en total veinte características que no deben ser consideradas como criterios para distinguir en el trato a las personas. Estas categorías –se especifica– podrían ser personales o colectivas, temporales o permanentes. Las categorías prohibidas, que siempre deben entenderse como ejemplificativas, reflejan preocupaciones de movimientos sociales que se visibilizan para ser protegidos y que históricamente han sido discriminados. Desde esta perspectiva, la enumeración, por grande que parezca, no es un agregado arbitrario o retórico[104].

Si bien ambos proyectos recogían las situaciones por las cuales la Constitución prohíbe que una persona pueda ser discriminada[105]; el PLODP 2019 introdujo, como una novedad, la protección y definición de los datos biométricos y genéticos. Por una parte, distinguió que los datos biométricos eran un "dato personal único obtenido a partir de un tratamiento técnico específico, relativo a las características físicas, fisiológicas o conductuales de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" –art. 5.4–; y por otra, precisó que los datos genéticos eran "un dato personal único relacionado a características genéticas heredadas o adquiridas de

[104] Ávila Santamaría, *Los derechos y sus garantías. Ensayos críticos*, 73.

[105] La Constitución señala que "nadie podrá ser discriminado por razones de etnia, lugar de nacimiento, edad, sexo, identidad de género, identidad cultural, estado civil, idioma, religión, ideología, filiación política, pasado judicial, condición socio-económica, condición migratoria, orientación sexual, estado de salud, portar VIH, discapacidad, diferencia física; ni por cualquier otra distinción, personal o colectiva, temporal o permanente, que tenga por objeto o resultado menoscabar o anular el reconocimiento, goce o ejercicio de los derechos" –art. 11.2–.

una persona natural que proporcionan información única sobre la fisiología o salud de un individuo“ –art. 5.5–. En este orden, identificamos que, en relación a los datos biométricos, la LOPD ha dejado de considerar que estos datos pueden obtenerse “*a partir de un tratamiento técnico específico”* –art. 4–. Una prescripción que sí está incluida en el RGDP. En todo caso, se ha conservado la misma definición relativa a los datos genéticos –art. 4–.

Dado que, en el RGPD, no se incluyen definiciones sobre el concepto de datos sensibles o especialmente protegidos –sí lo hace la Guía Legislativa de la OEA y los EPEI–; como pudimos evidenciar, su protección se encuentra garantizada en apartados específicos en los cuales se hace referencia a las excepcionalidades o criterios de legitimación para el tratamiento de esta categoría de datos[106]. Aun así, el RGPD define a los datos biométricos como datos “obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos” –art. 4.14–. Asimismo, precisa a los datos genéticos como datos “relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona” –art. 4.13–[107].

Hay que advertir que la LOPD recoge, prácticamente, las mismas definiciones que hace el RGPD, sobre datos biométricos y datos genéticos. Se trata de una

[106] Conviene señalar que la LOPD 15/1999 estimaba que “nadie podrá ser obligado a declarar sobre su ideología, religión o creencias” –art. 7.1–. Salvo con el consentimiento expreso y por escrito del afectado podían “ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias” –art. 7.2–. Así también sólo podían ser recabados, tratados y cedidos por razones de interés general, “los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual” –art. 7.3–; y en todo caso, quedaban prohibidos “los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual” –art. 7.4–.

[107] El RGPD aclara que esta tipología de datos está relacionada con “características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente” –Considerando 34–.

importante novedad, toda vez que, considerados como categorías especiales de datos personales, por una parte, "el estudio de los datos genéticos de una persona puede revelar datos íntimos de su propia configuración genética cuyo conocimiento por terceras personas o su divulgación pueden afectar de manera trascendente a su titular"[108]; y por otra, en el caso de los datos biométricos, su protección, "ha sido consecuencia de la particular importancia que han adquirido por la generalización de su utilización mediante sistemas informáticos de seguridad biométrica que tienen por objeto recopilar y valorar datos personales como huellas dactilares"[109].

#### 2.3.5 Disociación de datos (procedimiento de disociación y/o seudonimización)

Puede entenderse como todo procedimiento encaminado a asegurar que el tratamiento de la información personal imposibilite la identificación de una persona[110]. Según el Diccionario de la RAE la disociación significa la "acción y efecto de disociar la conexión entre el dato de carácter personal y su título, impidiendo su identificación". Esto es "separar algo de otra cosa a la que estaba unida". En el derecho a la protección de datos, "para que haya una autentica disociación es necesario que resulte imposible o requiera un plazo o requiera una actividad desproporcionada asociar un determinado dato con una persona

[108] José María Pérez Gómez, "Especialidades en el sector sanitario", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 198.
[109] Ibíd., 199.
[110] Al respecto, el RGPD señala que: "los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo" –Considerando 26–.

concreta”[111]. Así, la disociación o anonimización impide vincular los datos personales con una determinada persona, y se aplica, especialmente, en actividades relacionadas con “salud pública e investigación y, en muchas ocasiones, además, es una exigencia del principio de calidad y de proporcionalidad, porque estas actividades no requieren siempre el tratamiento de datos personales, teniendo en cuenta que se trata de datos especialmente protegidos”[112].

Conforme a lo expuesto, el PLODP 2016 estimó como disociación de datos al “procedimiento mediante el cual los datos personales no pueden vincularse a una persona determinada o determinable” –art. 4.5–[113]. Ahora bien, el PLODP 2019 distinguió la anonimización como “la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o re-identificación de una persona natural sin esfuerzos desproporcionados “–art. 5.1–. Esta definición que, finalmente, ha sido aceptada por el legislador en la LOPD –art. 4–. Al respecto, los EPEI apuntan que la disociación o anonimización es “la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados” –art. 2.1. a) –. De hecho, conforme señala la Guía Legislativa de la OEA, habrá que considerar que el concepto de “desidentificación” o “anonimización” describe el “derecho a omitir o suprimir información específica”[114]. No obstante, advertimos la necesidad de estar atentos a los procesos de disociación “porque, en ocasiones, utilizando la tecnología de *big data,* sin emplear un tiempo o un coste desproporcionado, una información aparentemente disociada, vinculada a

[111] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 478.
[112] Troncoso, “Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales”, 209.
[113] Al mismo tenor, la LOPD 15/1999 entendía que el procedimiento de disociación es “todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable” –art. 3.f)–.
[114] Como establece la Guía Legislativa de la OEA, “en algunos marcos reglamentarios nacionales y regionales se da a las personas el derecho a solicitar que los controladores de datos supriman (o borren) datos personales específicos que, aunque estén a disposición del público, las personas afirmen que ya no son necesarios o pertinentes”.

otros datos personales, puede convertirse en un dato de una persona identificable, siendo posible la re-identificación[115].

En este orden, el RGPD distingue que la seudonimización es el tratamiento de datos, de modo que, "ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable" –art. 4.5–. Prácticamente, es una definición que también ha sido acogida por la LOPD –art. 4–. Desde esta perspectiva, consideramos conveniente diferenciar la anonimización –incluida en ambos proyectos de Ecuador–, de la seudonimización –introducida, a partir de la aprobación de la LOPD–. Ambos términos, finalmente, concretados en la normativa de protección de datos que fue aprobada en mayo de 2021. Esta constituye una distinción necesaria, por cuanto:

> La seudonimización tiene que ser vista, desde dos perspectivas. Por una parte, es una exigencia del principio de calidad y de la prohibición de tratamientos excesivos que obliga a seudonimizar si puedo realizar la actividad sin datos de personas identificadas (…) Por otra parte, la seudonimización es junto con el cifrado las dos únicas medidas de seguridad del tratamiento de datos mencionadas expresamente en el art. 32.1.a) del RGPD. En general, la seudonimización abre la posibilidad a los encargados del tratamiento de realizar ciertas operaciones que no serían posible si los datos estuvieran cifrados. Por ello, le corresponde al responsable del tratamiento o, si existe una adhesión a un código de conducta a quien lo elabore, determinar si para garantizar la seguridad del tratamiento es suficiente la seudonimización o es necesario el cifrado[116].

El concepto de seudonimización constituye una medida de seguridad dentro del tratamiento de la información personal y, desde luego, una posibilidad de garantizar el principio de calidad, a partir de las actividades que cumplen los responsables y encargados[117]. "Persigue reducir los riesgos para los interesados y facilitar el

---

[115] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 209.

[116] Ibíd., 210, 211.

[117] Por ejemplo, el RGPD señala que "la aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos" –Considerando 28–; y así también que "para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente

cumplimiento de la normativa para los responsables y encargados. Esta finalidad, está en nuestra opinión, en la línea del principio de minimización de datos"[118]. En todo caso, por una parte, tomando en cuenta la LOPD –la cual sigue la línea del RGPD y de los EPEI– habrá que considerar que "la disociación o anonimización, que es definitiva y que impide la identificación de las personas afectadas, de manera que el tratamiento no entra dentro del ámbito de aplicación del RGPD –al no existir un tratamiento de datos personales–"[119]; y por otra que, los datos personales seudonimizados "deben considerarse información sobre una persona física identificable, mientras que los principios de protección de datos no deben aplicarse a la información anónima, es decir, información que no guarda relación con una persona física identificada o identificable, inclusive con fines estadísticos o de investigación"[120].

### 2.3.6 Habeas data (ejercicio de los derechos de acceso, rectificación, cancelación y oposición)

Mediante esta definición se pretende conceptualizar las facultades que garantizan el ejercicio de este derecho fundamental, por medio del *habeas data*[121]. Hacemos referencia a los derechos de acceso, rectificación, cancelación y oposición. Por una parte, la CCE reconoce que el *habeas data* y tiene por objeto "mantener el control de los datos que existan sobre una persona o sobre sus bienes, y para proteger el

Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas" –Considerando 29–.

[118] Arias Pou, "Definiciones a efectos del Reglamento General de Protección de Datos", 128.

[119] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 210.

[120] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 340.

[121] El octavo principio de la Guía Legislativa de la OEA sobre "acceso y corrección" señala que "en el ordenamiento jurídico interno de algunos países de las Américas (pero no en todos) se reconoce el derecho de *habeas data*, en virtud del cual las personas pueden entablar juicio para prevenir un presunto abuso de sus datos personales o ponerle fin. Ese derecho podría dar a la persona acceso a bases de datos públicas o privadas, así como el derecho a corregir los datos en cuestión, a mantener el carácter confidencial de los datos personales sensibles y a rectificar o borrar datos perjudiciales.

derecho a la honra, a la buena reputación y a la intimidad personal y familiar[122]; y por otra que, frente a ese control de la información, se posibilita "conocer el contenido de la misma y de ser el caso, exigir su actualización, rectificación, eliminación o anulación cuando aquella información le causan algún tipo de perjuicio, a efectos de salvaguardar su derecho a la intimidad personal y familiar[123].

Sobre la base de los derechos a la privacidad de la información personal y al libre desarrollo de la personalidad, destacamos que la Corte Interamericana de Derechos Humanos reconoce, además, la importancia de garantizar y respetar las facultades que se desprenden del *habeas data*. En este aspecto, la Corte precisa que:

> De conformidad con lo anterior, se puede concluir que el derecho de cada persona a definir de manera autónoma su identidad sexual y de género y a que los datos que figuran en los registros, así como en los documentos de identidad sean acordes o correspondan a la definición que tienen de sí mismos, se encuentra protegido por la Convención Americana a través de las disposiciones que garantizan el libre desarrollo de la personalidad (artículos 7 y 11.2), el derecho a la privacidad (artículo 11.2), el reconocimiento de la personalidad jurídica (artículo 3), y el derecho al nombre (artículo 18). Lo anterior significa que los Estados deben respetar y garantizar a toda persona, la posibilidad de registrar y/o de cambiar, rectificar o adecuar su nombre y los demás componentes esenciales de su identidad como la imagen, o la referencia al sexo o género, sin interferencias por parte de las autoridades públicas o por parte de terceros. En esa línea, lo expresado implica necesariamente, que las personas que se identifiquen con identidades de género diversas deben ser reconocidas como tal. Además, el Estado debe garantizarles que puedan ejercer sus derechos y contraer obligaciones en función de esa misma identidad, sin verse obligadas a detentar otra identidad que no representa su individualidad, más aún cuando ello involucra una exposición continua al cuestionamiento social sobre esa misma identidad afectando así el ejercicio y goce efectivo de los derechos reconocidos por el derecho interno y el derecho internacional[124].

---

[122] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 67-11-JD– publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.

[123] Véase la Resolución de la Corte Constitucional 182, Sentencia Nro. 182-15-SEP-CC –CASO Nro. 1493-10-EP– publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015. Esta misma resolución describe que la dimensión utilitaria de "*Habeas data* informativo" o "derecho de acceso" consiste en "la dimensión procesal que asume el *habeas data* para recabar información acerca del qué, quién, cómo y para qué se obtuvo la información considerada personal".

[124] Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-24/17 relativa a la identidad de género, e igualdad y no discriminación a parejas del mismo sexo, solicitada por la República de Costa Rica, 2017. Sobre este respecto, la Corte también destaca que "El sistema jurídico, debe evolucionar a la par de la sociedad y no puede desconocer los cambios que en ésta se operan, so pena de tornarse ineficaz. En este orden de ideas, respecto a los derechos humanos, la Ley debe mantener vigentes el alcance de las garantías y libertades reconocidas por la Convención y por el derecho interno. Así, corresponde a la Ley, regular nuevas maneras de ejercicio de los derechos humanos, estrechamente ligadas a los avances y desarrollos tecnológicos. Al igual que la función de configuración, las Leyes que actualizan indican significados, alcances, contenidos que en el momento en el que se creó el derecho no se previeron o simplemente no existían. Un ejemplo de ello sería el alcance de la libertad de expresión y el *habeas data* los cuales no eran imaginables hace 50 o 100 años atrás".

En este orden, los EPEI consideran que uno de los derechos de los titulares es el ejercicio de los derechos ARCO, mediante los cuales "el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales que le conciernen" –art. 24.1–; y en todo caso, "el ejercicio de cualquiera de los derechos referidos en el numeral anterior no es requisito previo, ni impide el ejercicio de otro" –art. 24.2–. En este caso, la Guía Legislativa de la OEA sugiere que es esencial la garantía de control de los datos, con el objeto de asegurar "su exactitud y pedir al controlador de datos que modifique, revise, corrija o elimine los datos en cuestión. Este derecho de acceso y corrección es una de las salvaguardias más importantes en el campo de la protección de la privacidad". Por esta razón, advertimos que:

> Si para hacer efectiva la facultad de decidir sobre la difusión y la utilización de nuestros datos personales es necesario poder conocer en cualquier momento quién los tiene, y a qué usos los destina, también resulta del todo imprescindible poder saber qué datos son en concreto, de dónde proceden y a quién se prevé comunicarlos. Es lo que se conoce como el derecho de acceso a los datos personales –que no hay que confundir con el derecho de acceso a los documentos públicos– y que, junto con los derechos de rectificación y de cancelación, hace posible ejercer el poder de disposición y control sobre los datos propios, característica fundamental del derecho a la autodeterminación informativa[125].

Ahora bien, el PLODP 2016 determinó que la protección de datos personales se definía como la "facultad que otorga la Ley para que el dueño de los datos personales, decida a quién proporciona su información, cómo y para qué. Este derecho permite acceder, rectificar, cancelar y oponerse al tratamiento de su información personal" –art. 4.6–. De esta disposición –que coincidía con algunos de los criterios que la jurisprudencia de la CCE–, observamos la deficiente redacción legislativa, en cuanto refiere al titular de los datos personales calificándolo como, "dueño de los datos personales". Ahora bien, en el PLODP 2019 los derechos ARCO eran vistos como parte de las facultades que se atribuyen al titular de los datos personales –a partir, del ejercicio de los derechos a la lealtad, transparencia e información–, estableciéndose que el titular tiene derecho a ser informado, de forma leal y transparente, sobre "la existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición,

[125] Ramon Oró, *La protección de datos*, 68.

anulación, limitación del tratamiento, y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas" –art. 23.14–. A la luz de la LOPD, el legislador ha considerado incluir este reconocimiento como parte del derecho a la información –art. 12.14–.

Aunque la protección de la información personal era tutelada, por medio de otros derechos –derecho a la intimidad o privacidad, por ejemplo–; recordemos que, frente a los avances y desarrollos tecnológicos de la sociedad, el *habeas data* ha estado relacionado con la protección de datos, mediante el aseguramiento y garantía de las facultades de control de la información. Por ello, "se reconocen como facultades integrantes del derecho a la protección de datos personales los derechos de acceso, rectificación y cancelación y se regula detalladamente lo relativo a la información y al consentimiento del titular de los datos"[126]. Con referencia a este aspecto, señalamos que en el PLOPD 2016 no existían definiciones relacionadas con el acceso y conocimiento, actualización y rectificación, como facultades del derecho a la protección de datos. Sin embargo, el PLODP 2019 sí las reconoció como parte de los derechos de los titulares de datos personales.

Entendiendo que el derecho de acceso "se origina a iniciativa del interesado, cuando solicita del responsable la información relativa al tratamiento de los datos"[127], el PLODP 2019 establecía que el derecho de acceso consistía en la facultad que tenía el titular de los datos para "conocer y obtener del responsable del tratamiento acceso a todos sus datos personales" y, así también "a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna" –art. 24–. En este punto, finalmente, la LOPD ha agregado que dicho acceso será gratuito y, por tanto, reconoce que "el titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna" –art. 13–.

[126] Arenas Ramiro, "La protección de datos personales en los países de la Unión Europea", 132.

[127] Javier Aparicio Salom, "Derechos del interesado (Arts. 12-19)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 377.

Se trata de una disposición similar a la que recoge el RGPD, por cuanto éste determina que el acceso es el "derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen" –art. 15.1–[128]; el derecho a ser informado de las garantías adecuadas "cuando se transfieran datos personales a un tercer país o a una organización internacional" –art. 15.2–; y además, el derecho a obtener copia "de los datos personales objeto de tratamiento" –art. 15.3–. Si bien el art. 13 de la LOPD no señala, expresamente, la obligación de informar en el caso de transferencias internacionales; esta norma se remite a su art. 12.10, en donde se establece el deber de informar sobre "las transferencias o comunicaciones, nacionales o internacionales, de datos personales, que se pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de éstas y las garantías de protección establecidas".

A diferencia del RGPD, por una parte, el PLODP 2019 no determinó que este derecho se asegure, a partir de la información sobre las garantías adecuadas en el caso de las transferencias de datos –art. 23.10–. En todo caso, como queda anotado, la LOPD ha completado esta disposición, reconociendo el deber de informar sobre las garantías de protección –art. 13–. Esta constituye una previsión necesaria, por cuanto "las características de los flujos de información y el carácter abierto de las redes posibilitan el acceso a los datos, así como su recopilación y tratamiento simultáneo en y desde varios países"[129], evidencian la obligación de

[128] Según el RGPD, se concederá el derecho de acceso a los datos personales y a la siguiente información: "a) los fines del tratamiento; b) las categorías de datos personales de que se trate; c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo; e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; f) el derecho a presentar una reclamación ante una autoridad de control; g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen; h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado" –art. 15–.

[129] Ortega Giménez, "La desprotección internacional del titular del de derecho a la protección de datos de carácter personal", 40.

ofrecer a las personas suficientes garantías, frente a intromisiones ilegítimas. Y por otra, expresamente, en el PLODP 2019 no existió referencia al derecho a obtener copia de los datos personales, por el cual se garantiza que "los datos deben facilitarse al interesado en un formato de lectura accesible, de forma que pueda conocer y entender cuál es la información que se somete a tratamiento"[130]. No obstante, tanto el PLODP 2019 –art. 24– como la LOPD –art. 13– han prescrito que "el responsable del tratamiento deberá establecer métodos razonables que permitan el ejercicio de este derecho".

En lo que corresponde al derecho de rectificación, éste "legitima al interesado a exigir del responsable del tratamiento que el tratamiento de los datos sea fiel reflejo de la realidad, actualizando los datos cuando éstos resulten inexactos o incompletos"[131]. Bajo este supuesto, el PLODP 2019 estableció que, mediante el derecho de rectificación y actualización, "el titular tiene el derecho de solicitar se corrijan o actualicen sus datos inexactos, incompletos, desactualizados, erróneos, falsos, incorrectos o imprecisos" –art. 25–. Finalmente, la LOPD ha concretado que este derecho implica que "el titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos" –art. 14–. Se trata de una disposición parecida a la del RGPD, por cuanto éste garantiza que "el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional" –art. 16–. Con relación al RGPD, la única diferencia que encontramos es que la LOPD no determina que la solicitud de rectificación pueda hacerse, por medio de una declaración adicional, lo cual implica un nuevo derecho del titular de los datos, garantizando "la capacidad de exigir del responsable del tratamiento que complete los datos sometidos a tratamiento con información adicional, es decir que se añada al tratamiento de los datos la información que interese aportar al interesado"[132].

[130] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 386.
[131] Ibíd., 388.
[132] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 389.

Por otra parte, el derecho de cancelación o de supresión faculta al interesado "a exigir del responsable del tratamiento que excluya del tratamiento los datos de carácter personal que resulten innecesarios para el fin que justificó el tratamiento, por no interesarle que se sometan a tratamiento"[133]. En este marco, el art. 26 del PLODP 2019 ha materializado en la LOPD esta facultad en el derecho de eliminación, por el cual "el titular tiene derecho a que el responsable del tratamiento suprima sus datos personales" –art. 15–[134]. La propuesta coincide con el RGPD, en tanto reconoce el derecho del interesado a obtener "del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida" –art. 17.1–[135]; y, en cuanto a que la LOPD establece que el responsable del tratamiento deberá cumplir con esta obligación "en el plazo de quince (15) días de recibida la solicitud por parte del titular y será gratuito" –art. 15–. Esta ha sido una incorporación oportuna que ha realizado el legislador, tomando en cuenta que no estaba prescrita en el art. 26 del PLODP 2019. Así, el hecho de que la supresión implique el derecho del interesado a obtener la cancelación de sus datos sin dilación indebida significa, por una parte, prevenir en el tiempo mayores riesgos, afectaciones o intromisiones sobre el derecho a la

[133] Ibíd., 390.

[134] La LOPD determina que este derecho se ejercerá cuando: "el tratamiento no cumpla con los principios establecidos en la presente Ley" –art. 15.1–; "el tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad" –art. 15.2– ; "los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados" –art. 15.3–; "haya vencido el plazo de conservación de los datos personales" –art. 15.4–; "el tratamiento afecte derechos fundamentales o libertades individuales" –art. 15.5–; "revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, si necesidad de que medie justificación alguna" –art. 15.6–; y, finalmente, "exista una obligación legal" –art. 15.7–.

[135] En este caso, el RGPD señala que procede el derecho a la supresión cuando: "a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1" –art. 17.1–.

protección de datos; y por otra, garantizar que el ejercicio de esta facultad se cumpla dentro de un plazo razonable.

Hay que considerar que, reforzando o extendiendo el derecho de supresión, encontramos el derecho al olvido "que permite a las personas eliminar las referencias a algunos hechos de su vida que aparecen reflejados en Internet y que, con independencia de su origen y de si son verdaderos o no, podrían afectar a su desarrollo ulterior como personas"[136]. Este derecho que ha sido una de las principales innovaciones del RGPD[137], también se encontraba considerado en el PLODP 2019. No obstante, el legislador desaprovechó esta propuesta para dejar de incluirla en el texto final que aprobó la LOPD. En todo caso, consideramos conveniente conceptualizar, brevemente, el alcance que tiene este derecho a la luz de la normativa de protección de datos personales.

Así, bajo el concepto de derecho al olvido digital, el PLODP 2019 consideraba que "el titular tiene el derecho a solicitar al juez competente, obtener sin dilación indebida del responsable del tratamiento la supresión de sus datos personales que estén siendo tratados en el entorno digital" –art. 27–. Al respecto, el RGPD determina que esta extensión del derecho de supresión es ejercida ante el responsable del tratamiento, en donde éste "teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos" –art. 17.2–[138].

[136] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 394.

[137] Precisamente, el RGPD advierte que "a fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales" –Considerando 66–.

[138] El RGPD añade que el derecho a la supresión de datos o derecho al olvido, no se aplicará cuando el tratamiento sea necesario: "a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el

Llamaba la atención que, en la propuesta de Ecuador, la solicitud debía ser planteada ante el juez competente y, no frente al responsable del tratamiento. No encontrábamos justificación para que no pudiera ser ejercido frente al responsable, por cuanto el derecho al olvido sirve para que el titular de los datos personales exija, directamente, "a los editores de los contenidos que publican información personal la supresión de tales contenidos y la notificación a los motores de búsqueda del derecho de supresión ejercido frente a ellos. De esta forma, los buscadores dejarán de indexarlos y de incluirlos en la lista de resultados"[139].

Finalmente, el derecho de oposición se plantea como "el medio de protección en los casos en que el responsable del tratamiento procesa los datos personales para la realización de un interés público o cuando invoca un interés legítimo como fundamento del tratamiento"[140]. En el PLODP 2019, este derecho suponía, de manera general, que el titular pudiera oponerse o negarse "al tratamiento de sus datos personales, en especial para fines de mercadotecnia, valoraciones o decisiones automatizadas incluida la elaboración de perfiles" –art. 28–. En este punto, el RGPD refiere que la oposición tendrá lugar "en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones" –art. 21.1–[141]; "cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa" –art. 21.2–; cuando se utilicen "en el contexto de la

Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones" –art. 17.3–..

[139] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 396.

[140] Javier Aparicio Salom, "Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 409.

[141] El RGPD añade que "el responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones" –art. 21–.

utilización de servicios de la sociedad de la información" –art. 21.5–; y "cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos" –art. 21.6–.

En cualquier caso, la LOPD ha decidido seguir la línea del RGPD, por cuanto entiende que este derecho faculta a que "el titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos: "no se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley" –art. 16.1–; "el tratamiento de datos personales tenga por objeto la mercadotecnia directa –art. 16.2–; "cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, previsto en el artículo 7" –art. 16.3–. En este marco, al igual que el RGPD, observamos que la LOPD "atribuye al interesado la capacidad de impedir el tratamiento basado en el interés público, el interés legítimo y el tratamiento, cualquiera que sea su fundamento, cuya finalidad sea la publicidad (mercadotecnia) directa"[142].

#### 2.3.6.1 Limitación al tratamiento, portabilidad y decisiones individuales automatizadas

En primer término, la limitación al tratamiento "consiste en que el interesado pueda pedir al responsable del tratamiento que utilice medios técnicos de forma que los datos personales no sean objeto de operaciones de un tratamiento ulterior determinado ni puedan modificarse"[143]. Es definida por el RGPD como "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro" –art. 4.3–. Esta definición, se restringe, exclusivamente, a "establecer la forma de llevarlo a cabo (incrustando en los datos alguna señal o distintivo que

[142] Aparicio Salom, "Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23)", 410.
[143] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 341.

impida su tratamiento) y no presta atención, sin embargo, a las causas o propósitos de dicha limitación, a salvo de indicar que sólo es limitación el supuesto en que el marcado de los datos persigue la finalidad de evitar el tratamiento ulterior"[144].

Si bien, el art. 5 del PLODP 2019 no realizaba una definición sobre este concepto, dentro del régimen jurídico relativo a los derechos del titular de datos personales se determinaba que la limitación del tratamiento garantizaría que el titular tiene derecho a que: "se use el mínimo de sus datos personales en el tratamiento efectuado por responsables o encargados del tratamiento"; "sus datos personales no se encuentren disponibles en Internet u otros medios de comunicación masiva"; "el tratamiento de datos se limite al período que medie entre una solicitud de revisión de juridicidad, lealtad, transparencia, legitimidad, acceso, eliminación, rectificación y actualización, oposición, anulación, portabilidad, limitación del tratamiento, o de no ser objeto de una decisión basada únicamente en valoraciones automatizadas" –art. 32–. Ahora bien, en la LOPD el legislador ha considerado que la limitación al tratamiento se identifique como el derecho a la suspensión –art. 19–, a partir de algunas condiciones. Por ejemplo, cuando: "el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos" –art. 19.1–; "el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso" –art. 19.2–; "el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones" –art. 19.3–; y "cuando el interesado se haya opuesto al tratamiento en virtud del artículo 31 de la presente ley, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado" –art. 19.4–.

Evidentemente, la LOPD adopta la regulación que propone el RGPD, por el cual se reconoce el derecho del interesado a "obtener del responsable del tratamiento la limitación del tratamiento de los datos" –art. 18.1–, cuando se cumplan los siguientes supuestos:

[144] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 397.

> a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

En ambos casos, advertimos que:

> El derecho a la limitación de los datos se regula como un derecho del interesado y no como una obligación del responsable. Esta circunstancia plantea, de entrada, la duda de si el responsable del tratamiento tiene la obligación de limitar el tratamiento tan pronto como concurre alguna de las circunstancias que hacen nacer este derecho, o si, por el contrario, las causas que dan lugar a este derecho simplemente legitiman al interesado a instar del responsable que proceda a la limitación y, si el interesado no lo solicita, el responsable puede continuar con el tratamiento de los datos a pesar de que haya concurrido dicha circunstancia e incluso, sea consciente de ella[145].

Por tanto, concluimos que "el responsable del tratamiento sólo tiene la obligación de llevar a cabo la limitación cuando el interesado se lo solicita"[146], ejerciendo los supuestos que se plantean en el art. 19 de la LOPD. Finalmente, conviene señalar que, cuando el tratamiento de datos se haya limitado conforme a los supuestos señalados, el RGPD establece que dichos datos solo podrán ser objeto de tratamiento, "con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante" –art. 18.2–; y, además, que el interesado "será informado por el responsable antes del levantamiento de dicha limitación" –art. 18.3–. Estas disposiciones se encontraban ausentes en el PLODP 2019. No obstante, la LOPD ha introducido en el art. 19 *in fine* que, a partir del ejercicio del derecho a la suspensión del tratamiento, el responsable podrá tratar los datos personales, únicamente, en los siguientes supuestos: "para la formulación, el ejercicio o la defensa de reclamaciones; con el objeto de proteger los derechos de otra persona natural o jurídica o por razones de interés público importante". En todo

[145] Ibíd., 398.

[146] Ibíd.

caso, consideramos esencial manifestar que el legislador ha olvidado prescribir y garantizar la obligación de informar.

Ahora bien, el derecho a la portabilidad de los datos "se identifica como un instrumento que puede dotar a las personas, cuyos datos son objeto de tratamiento, de un mayor control sobre los mismos"[147]. Así, el RGPD reconoce que el interesado "tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado" –art. 20.1–. En este mismo sentido, el art. 30 del PLODP 2019 concretó en la LOPD que el titular de los datos "tiene derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, inter-operable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables" –art. 17–. En este caso, es necesario advertir que no puede confundirse el derecho de acceso con el derecho de portabilidad, por cuanto "la portabilidad se distingue del acceso en que aquélla garantiza al interesado la obtención de una copia de la información susceptible de ser procesada sin dificultad, mientras que el acceso se limita a garantizar la información en sí misma"[148].

El RGPD aclara que este derecho procede cuando el tratamiento: "esté basado en el consentimiento" –art. 20.1. a)–; y "se efectúe por medios automatizados" –art. 20.1. b)–; recordando que, además, "el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible" –art. 20.2–. Estos mismos supuestos –a la luz del art. 30 del PLODP 2019– se encuentran recogidos en la LOPD, cuando se establece que la

[147] Ramón Miralles López, "Derecho de portabilidad (Art. 20)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 401. En este aspecto, además manifestamos que "el ejercicio del derecho de acceso incluye la posibilidad de conocer qué datos concretos maneja el responsable del tratamiento, pudiéndose obtenerse esa información por diferentes vías: visualización en pantalla; escrito, copia o fotocopia enviada por correo, certificado o no; telecopia; correo electrónico u otros sistemas de comunicaciones electrónicas; y cualquier otro sistema que pueda ofrecer el responsable del tratamiento". Cfr. Miralles López, "Derecho de portabilidad (Art. 20)", 402.
[148] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 386.

portabilidad procede, siempre y cuando cumpla, al menos una de las siguientes condiciones, a saber: “que el titular haya otorgado el consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos” –art. 17.1–; “que el tratamiento se efectúe por medios automatizados” –art. 17.2–; “que se trate de un volumen relevante de datos personales” –art. 17.3–; y “que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento, o del titular en el ámbito del derecho laboral y seguridad social” –art. 17.4–.

Ahora bien, en cuanto a la posibilidad de que los datos personales se transmitan, directamente, de responsable a responsable; el PLODP 2019 señalaba que el titular podía “solicitar la transferencia o comunicación de sus datos personales a otro responsable del tratamiento” –art. 30–, sin advertir las posibles limitaciones técnicas. En todo caso, la LOPD ha complementado la propuesta de 2019, manifestando que dicha transferencia aplicará “en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de ralentizar el acceso, la transmisión o reutilización de datos por parte del titular o de otro responsable del tratamiento” –art. 17–.

De esta manera, el derecho a la portabilidad:

> Nos acerca más al hecho de que los datos de carácter personal no le pertenecen al responsable del tratamiento, ya que ahora la persona cuyos datos están siendo objeto de tratamiento dispone de un instrumento que le permite recuperarlos «físicamente», avanzando a un nivel superior de control sobre sus datos, como sería la posesión y movilidad respecto de sus datos y, en consecuencia, ciertos desequilibrios entre usuarios y proveedores de servicios se pueden ver corregidos[149].

Además, según el RGPD, el ejercicio del derecho a la portabilidad de los datos se entenderá sin perjuicio del derecho de supresión o derecho al olvido y, en todo caso, “no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento” –art. 20.3–[150]. Si bien el art. 17 *in fine* de la LOPD

[149] Miralles López, “Derecho de portabilidad (Art. 20)”, 403.

[150] El RGPD advierte, además, que el derecho a la portabilidad de los datos “no afectará negativamente a los derechos y libertades de otros” –art. 20.4–. Al respecto, señalamos que esta

determina que este derecho no procede “cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el titular”. La limitación que advierte el RGPD se encuentra ausente en la LOPD. Por ello, admitimos la necesidad de garantizar que “los datos relacionados con los tratamientos responsabilidad de las administraciones públicas en el ejercicio de las funciones y competencias que les son propias, no podrán ser solicitados para su entrega en las condiciones que prevé el derecho a la portabilidad”[151].

Por último, en relación al derecho sobre decisiones individuales automatizadas, se trata de una especificación del derecho de oposición, que se refiere “a la singularización del tratamiento con los individuos y la analítica de comportamiento para la obtención de perfiles que permiten aplicar decisiones singulares basadas en las conclusiones extraídas del análisis del comportamiento”[152]. Así, el RGPD garantiza el derecho a “no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar” –art. 22.1–[153]. La

prescripción se encontraba garantizada en el art. 1 del PLODP 2019, cuando se reconocía que la Ley regulará el ejercicio del derecho a la protección de datos personales, la autodeterminación informativa y demás derechos digitales en el tratamiento y flujo de datos personales, lo cual suponía, evidentemente, el respeto de los derechos y libertades de otras personas, dentro del tratamiento de datos. Como hemos precisado en el inicio de este capítulo, esta propuesta era mucho más completa y se adecuaba a las exigencias que plantea el derecho a la protección de datos. Por ello, enfatizamos en que el legislador ha restringido el reconocimiento de la protección de derechos y libertades, que puedan afectar a terceras personas. En todo caso, a la luz del paradigma del Estado constitucional de derechos y justicia, en Ecuador, habrá que considerar que: “ninguna norma jurídica podrá restringir el contenido de los derechos ni de las garantías constitucionales” –art. 11.4–; “en materia de derechos y garantías constitucionales, las servidoras y servidores públicos, administrativos o judiciales, deberán aplicar la norma y la interpretación que más favorezcan su efectiva vigencia –art. 11.5–; y, además, “todos los principios y los derechos son inalienables, irrenunciables, indivisibles, interdependientes y de igual jerarquía” –art. 11.6–.

[151] Miralles López, “Derecho de portabilidad (Art. 20)”, 405.

[152] Aparicio Salom, “Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23)”, 410.

[153] Según expone el RGPD, este supuesto no se aplicará si la decisión: “a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del

LOPD –sobre la base del art. 33 del PLODP 2019– sigue esta línea, ya que reconoce el derecho a "no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales" –art. 20–[154]. Se trata de una importante disposición que regula el derecho de oposición, frente al denominado big data, por cuanto éste –producto de la revolución digital– ha posibilitado "conservar toda la información relativa a cualquier experiencia y recuperar fácilmente los datos que interesan de forma ordenada y extraer mediante su estudio automático conclusiones que antes eran imposibles de conseguir"[155].

Además, la LOPD, basada en la propuesta del art. 33 del PLODP 2019, ha resuelto continuar con la dirección del RGPD, en cuanto a la determinación de las reglas por las cuales no se aplica este derecho. En este caso, la LOPD estatuye que no se aplicará si la decisión: "es necesaria para la celebración o ejecución de un contrato entre el titular y el responsable o encargado del tratamiento de datos personales" –art. 20.1–; "está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad técnica competente, para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y

interesado" –art. 22.2–. Así también aclara que en los casos "a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión" –art. 22.3–. Finalmente, advierte que "las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado" –art. 22.4–.

[154] Tanto el art. 4.4 del RGPD como el art. 4 de la LOPD entienden que la elaboración de perfiles comprende todo tratamiento automatizado destinado a evaluar, analizar o predecir aspectos de una persona, los cuales tienen relación con el rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación o movimientos físicos. De este modo, "el legislador es consciente de que el concepto de dato de carácter personal ha evolucionado y hoy en día es posible utilizar mecanismos que nos den información acerca de usos e intereses de un usuario, sin necesidad de conocer sus datos identificativos, lo cual, combinado con el uso de herramientas técnicas que permiten operaciones de tratamiento a gran escala lo que podría afectar a un gran número de interesados y entrañar probablemente un alto riesgo". Cfr. Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 341.

[155] Aparicio Salom, "Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23)", 413.

libertades del titular" –art. 20.2–; "se base en el consentimiento explícito del titular" –art. 20.3–; y, por último, "no conlleve impactos graves o riesgos verificables para el titular" –art. 20.4–.

En lo que corresponde a la LOPDGDD, sobre el ejercicio de los derechos antes mencionados, señalamos que –de conformidad a lo establecido en el RGPD– estos se ejercen por regla general "directamente o por medio de representante legal o voluntario" –art. 12.1–[156]. En todo caso, el responsable del tratamiento "estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden" –art. 12.2–; y además, se reconoce la garantía de gratuidad en "las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos" –art. 12.7–[157].

Bajo estas consideraciones, a diferencia del proyecto normativo de 2016, debe señalarse que el PLOPD 2019 presentó definiciones más completas y acordes a estándares internacionales, las cuales han sido adoptadas por el legislador en la LOPD aprobada en mayo de 2021.

Como se evidenciará en el siguiente capítulo, si bien en el PLOPD 2016 se hizo referencia a los derechos vinculados con el acceso y conocimiento, actualización y

[156] La LOPD 15/1999 reconocía dentro del principio de calidad de datos que, si los datos personales "resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16" –art. 4.4–. Incluso, más allá de lo que contemplaba el art. 16 sobre el derecho rectificación y cancelación –serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos–; también se destacaba la tutela del derecho de acceso que garantizaba al interesado el derecho a "solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos" –art.15.1–.

[157] Sobre este último aspecto, el RGPD advierte que deberán "arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas" –Considerando 59–. En este mismo sentido, los EPEI reconocen que "el responsable establecerá medios y procedimientos sencillos, expeditos, accesibles y gratuitos que permitan al titular ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad" –art. 32.1–.

rectificación, en esta propuesta no existieron definiciones sobre la naturaleza de dichas facultades, las cuales disponen un conjunto de garantías, relativas a el ejercicio del derecho a controlar que el tratamiento cumpla con los principios de la legislación de protección de datos personales. En suma, es importante considerar las facultades que se desprenden del concepto del *habeas data*, por cuanto ésta comprende un catálogo de derechos, facultades y obligaciones que precisa garantizar los derechos de acceso, rectificación, cancelación, oposición, limitación del tratamiento y portabilidad, como salvaguardias dentro del tratamiento de datos.

### 2.3.7 Responsable del tratamiento de la información

Tanto el responsable como el encargado del tratamiento constituyen definiciones esenciales dentro del derecho a la protección de datos. Por ello, sigue siendo importante "determinar en cada caso *quién decide* la finalidad del tratamiento, su contenido y su uso, a quién le corresponde la dirección y el control sobre el tratamiento de datos personales"[158]. El RGPD define el responsable del tratamiento como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento" –art. 4.7–[159]. Asimismo, según los EPEI es la persona "física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales" –art. 2.1. g)–. Por otra parte, en calidad de controlador de los datos, –siguiendo la definición de la Guía Legislativa de la OEA–, se encarga del almacenamiento, procesamiento, uso, protección y difusión de los

[158] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 341.

[159] La Guía Legislativa de la OEA precisa que el "responsable del tratamiento" tiene la calidad de "controlador de datos", de tal suerte que: "significa la persona física o jurídica, entidad privada, autoridad pública u otro organismo u organización que (solo o junto con otros) se encarga del almacenamiento, el procesamiento, el uso, la protección y la difusión de los datos en cuestión. En general abarca las personas físicas o jurídicas o las autoridades facultadas por las Leyes nacionales para tomar decisiones con respecto al contenido, el propósito y el uso de un archivo de datos o una base de datos. En algunas circunstancias, esta frase se aplica también a entidades que pueden describirse como "recopiladores de datos", ya que, en la mayoría de los casos, la entidad que almacena, usa y difunde los datos personales también se encarga (de manera directa o indirecta) de recopilarlos".

datos personales. Así, el responsable constituye un verdadero controlador de datos. El almacenamiento, procesamiento, propósitos, uso y más disposiciones relativas a garantizar la protección de la información personal se definen por el responsable, con el objeto de que el tratamiento de datos responda a los principios básicos de legitimidad y pertinencia o, en sentido más amplio, al principio de calidad de datos.

En este marco, el PLODP 2016 determinaba que el responsable del tratamiento constituía la "persona natural o jurídica, pública o privada que sola o conjuntamente con otros, administra el sistema de tratamiento de datos personales por cuenta del responsable del archivo, registro, base o banco de datos" –art. 4.7–. Asimismo, el PLODP 2019 lo definía como la "persona natural o jurídica, pública o privada, que decide sobre la finalidad y el tratamiento de datos personales" –art. 5.18–. A diferencia del RGPD, esta definición no especifica que el responsable también podía ser considerado una autoridad pública, servicio o cualquier organismo.

Ahora bien, el art. 4.7 *in fine* del PLODP 2016 justificaba, únicamente, la protección y salvaguardia de la identidad[160]. Sobre esta cuestión, insistimos que el derecho a la protección de datos constituye un instituto de garantía de otros derechos fundamentales y, por tanto, en el tratamiento de datos no podrían resultar afectados, solamente, bienes jurídicos vinculados con la identidad sino también derechos relacionados con la intimidad, el honor y dignidad de las personas. Además, si bien el PLODP 2016, se orientaba a describir una serie de prescripciones para el responsable del tratamiento –que debían enmarcarse en los derechos y garantías previstas para este derecho fundamental–; subrayamos que, el PLODP 2019 sintetizó la naturaleza del responsable, considerándolo como la "persona natural o jurídica, pública o privada que decide sobre la finalidad y el tratamiento de datos

[160] Con referencia a este punto, el PLOPD 2016 agregaba que "toda operación de información que comprometa datos personales en procedimiento mecánico o automatizado que tenga como fin la recolección, ordenamiento, conservación, almacenamiento, modificación, evaluación, destrucción, procesamiento de datos, así como el acceso de terceros por cualquier medio, deberá observar estrictamente la normativa prevista, bajo los derechos de protección y salvaguardia de identidad" –art. 4.7–.

personales" –art. 5.18–[161]. En todo caso, acogiendo la definición que realiza el RGPD, la LOPD entiende como responsable a la "persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales" –art. 4–. En este orden, el responsable "es el que tiene una cierta autonomía que le permite tomar las principales decisiones en cuanto al tratamiento de datos personales y en relación con el cumplimiento de los principios y el ejercicio de los derechos"[162]. En definitiva, es la persona que decide las reglas por las cuales se efectuará el tratamiento de la información, en cuanto al propósito, contenido y uso de los archivos, ficheros y bases o bancos de datos.

### 2.3.8 Encargado del tratamiento

Como hemos señalado, es importante aclarar la diferencia entre el encargado del tratamiento y el responsable tratamiento. Así, advertimos que el encargado "se limita a llevar a cabo el tratamiento de datos personales para el desarrollo de la gestión encomendada, cumpliendo en todo momento las instrucciones del responsable"[163].

El RGPD lo define como "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento" –art. 4.8–. Asimismo, los EPEI señalan que es el "prestador de servicios, que, con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste" –art. 2.1. e)–[164]. Bajo estas consideraciones, el PLODP 2016 no refirió una

[161] Al igual que la normativa europea, las propuestas de Ley y la LOPD en Ecuador; la LOPD 15/1999 consideraba que el responsable del tratamiento constituía "la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento" –art. 3.d)–.
[162] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 342.
[163] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 342.
[164] Puede también tomarse como referencia la definición fijada por la Guía Legislativa de la OEA donde el "encargado" tiene la calidad de "procesador de datos" de tal suerte que se refiere "a la persona física o jurídica, entidad privada, autoridad pública u otro organismo u organización que (solo o junto con otros) procesa los datos en cuestión. Por lo general, el procesador de datos es diferente del recopilador de datos. En algunos casos, el controlador de datos podría ser también el

definición relacionada con el encargo del tratamiento y, al parecer, atribuía esta categoría al "responsable del archivo, registro, base o banco de datos" definiéndolo como la "persona natural o jurídica, pública o privada que es titular de un archivo, registro, base o banco de datos como custodio y operador de la información" –art. 4.8–. No obstante, el PLODP 2019 definió, acertadamente, al encargado del tratamiento como a la "persona que trate datos personales por nombre y a cuenta de un responsable de tratamiento de datos personales" –art. 5.13–[165]. Como ha sucedido con la definición del responsable del tratamiento, es conveniente precisar que la LOPD ha resuelto vincular al encargado en los términos fijados por el RGPD. Así, la nueva normativa de protección datos manifiesta que es la "persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales" –art. 4–.

Finalmente, consideramos pertinente advertir que el PLODP 2016 confundió a la figura del encargado con la del responsable y, además, erróneamente, otorgó la titularidad del archivo al encargado del tratamiento. Por esta razón, aclaramos que, en el derecho a la protección de datos, el titular de la información personal –contenida en soportes físicos o automatizados, que identifique o haga identificable a una persona– es el interesado o, simplemente, titular de los datos. Por ello, la terminología que supuso aplicar el PLODP 2016 pudo dar lugar a confusiones. Tal como se advierte en la legislación comparada, el responsable es, simplemente, responsable y el encargado, meramente, encargado, y no responsable a la vez.

### 2.3.9 Titular de los datos

procesador de datos o podría efectuar arreglos para que otros se ocupen del procesamiento sobre la base de una relación contractual. La frase "procesamiento de datos" se usa en un sentido amplio y abarca toda operación o conjunto de operaciones realizado con datos personales, como recopilación, registro, almacenamiento, alteración, recuperación, divulgación o transferencia".

[165] Una definición parecida a esta propuesta estaba contenida en la LOPD 15/1999, la cual definía al encargado del tratamiento como "la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento" –art. 3.g)–.

El derecho a la protección de datos "nace para atribuir un control sobre los propios datos frente a los tratamientos tanto manual-estructurados como automatizados, aunque sean estos últimos los que presentan más peligros para los derechos fundamentales"[166]. A partir de la evolución de las tecnologías de la información y comunicación, proteger y tutelar los derechos inherentes al titular de los datos en la era de Internet, representa una constante preocupación debido a que, en el contexto jurídico, debe converger el desarrollo integral de las libertades fundamentales con el aseguramiento del ejercicio pleno de controlar sus propios datos. Así, subrayamos que "el titular del derecho a la protección de datos se encuentra en una evidente situación de inferioridad jurídica, que le sitúa al borde de la desprotección frente al superior conocimiento técnico y poder económico de los infractores"[167].

Respecto a este concepto, el RGPD refiere que el interesado o titular de los datos es toda "persona física" que resulte "identificada o identificable" dentro del tratamiento de la información personal" –art. 4.1–[168]. Así también los EPEI como la "persona física a quien le conciernen los datos personales" –art. 2.1. h)–; y la Guía Legislativa de la OEA como la "persona cuyos datos personales se recopilan, procesan, almacenan, utilizan o difunden". En tales circunstancias, como señala la CCE, el derecho a la protección de datos está supeditado a la existencia de "información que atañe a determinado sujeto y a la necesidad de que este tenga

[166] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 32.
[167] Ortega Giménez, "La desprotección internacional del titular del de derecho a la protección de datos de carácter personal", 54.
[168] Al respecto, el RGPD amplía que "los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo, los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento" –Considerando 63–.

una esfera mínima de actuación libre respecto de dicha información, sobre la cual no debería existir una interferencia ilegítima por parte de terceros"[169].

El objeto de este derecho es asegurar que el tratamiento de la información se haga de manera adecuada, salvaguardando los derechos y libertades que se desprenden de este instituto de garantía. En suma, proteger al titular de los datos, atribuyéndole el derecho a controlar su información, frente al tratamiento. Naturalmente, "esto se logra mediante un juego contrapuesto de atribución de derechos para el titular de los datos y de imposición de obligaciones para aquellos que captan o procesan los mismos y/o ejercen un control sobre dicho tratamiento de datos"[170]. Por tanto, al concederse al titular de los datos personales la facultad de controlar el tratamiento de la información, dicha atribución se perfecciona, mediante la garantía del *habeas data* –en virtud de sus dimensiones utilitarias y carácter instrumental–, que permite ejercer los derechos de acceso, rectificación, cancelación y oposición. Como señala la CCE, esta garantía sirve para tutelar el derecho a la seguridad jurídica de los ciudadanos. Por ende, asegura las facultades de control de la información. Así se entiende, cuando la Corte señala que esta garantía tiene el objeto de "proteger al ciudadano en caso de que el Estado o los particulares hagan uso de una información incorrecta, inexacta u obsoleta y que, al difundir tal información, se produzcan discrímenes, calificaciones deshonrosas, etc."[171].

Desde esta perspectiva, tanto el art. 4.9 del PLODP 2016 como el art. 5.21 del PLODP 2019 describían al titular de los datos como la "persona natural cuyos datos personales son objeto de tratamiento"[172]. Es decir, ambos proyectos concluyeron que dicho tratamiento era objeto de recopilación, almacenamiento, procesamiento, uso y difusión de la información personal. Lógicamente, se trató de una definición

[169] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 67-11-JD– publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.
[170] Ortega Giménez, "La desprotección internacional del titular del de derecho a la protección de datos de carácter personal", 38.

[171] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-09-SEP-CC –CASO Nro. 14-9-EP– publicada en el Registro Oficial Nro.18 de 3 de septiembre de 2009.
[172] En nuestro concepto, estas definiciones siguen la línea de LOPD 15/1999, la cual consideraba como afectado o interesado a la "persona física titular de los datos que sean objeto del tratamiento" –art. 3. e)–.

que ha sido aceptada por el legislador en la LOPD –art. 4–. En todo caso, cuando la normativa de protección de datos en Ecuador refiere como titulares de los datos personales a las personales naturales o físicas –excluyendo de su ámbito de aplicación material a las personas jurídicas, atendiendo el art. 2. g)–; recordemos que la CCE señala que:

> Por las características del derecho a la protección de datos personales, no se considera constitucionalmente adecuada la limitación a la calidad de las personas jurídicas como titulares del mismo; sin embargo, la información personal de dichos sujetos únicamente se extiende a las personas asociadas o a sus representantes legales, en tanto a la calidad que ostentan respecto de la persona jurídica, con estricto respeto al derecho a la protección de los datos personales y derechos conexos que le son atinentes a su naturaleza[173].

Como sabemos, en el ámbito internacional el RGPD regula la protección de datos de las personas físicas o naturales y excluye a las personas jurídicas[174]. De igual manera, en el caso de los tratamientos de datos relacionados con los empresarios individuales y los profesionales liberales "cuando se refieran a ellos únicamente en dicha condición puedan ser necesarios para la satisfacción de un interés legítimo perseguido por el responsable del tratamiento o por un tercero"[175]; puede considerarse como un supuesto de licitud de tratamiento de datos personales. En este sentido, finalmente, la LOPD ha prescrito que son accesibles al público y susceptibles de tratamiento los datos personales relacionados con "el contacto de profesionales y los datos de comerciantes, representantes y socios y accionistas de personas jurídicas y servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica y número de teléfono profesional. En el caso de los servidores públicos, además serán de acceso público y susceptibles de tratamiento

[173] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 67-11-JD– publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.

[174] El RGPD señala que "el presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto" –Considerando 14–.

[175] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 203.

de datos, el histórico y vigente de la declaración patrimonial y de su remuneración" –art. 2. g)–.

### 2.3.10 Tratamiento de datos

El tratamiento, procedimiento, método o sistema de administración de la información de carácter personal comporta uno de los aspectos más esenciales, dentro de la tutela del derecho a la protección de datos personales. Como señalan los EPEI, el tratamiento es "cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales"; las cuales están vinculadas con "la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales" –art. 2.1. i)–.

Tomando en cuenta que los datos personales pueden ser objeto de tratamiento, incluso, en el ámbito internacional, "la necesidad de regular adecuadamente este fenómeno es innegable; del mismo modo en que no caben dudas acerca de la complejidad de dicha tarea, dada la difícil conciliabilidad de intereses tan dispares como la protección de la intimidad personal, las legítimas aspiraciones comerciales de las empresas involucradas en el tratamiento internacional de datos, y la libertad de información y comunicación"[176]. Así, concluimos que, "el riesgo no proviene tanto de la existencia de información personal, sino de los tratamientos de datos personales"[177] y, por tanto, corresponde un "*manejo responsable*" de la información en las entidades públicas y privadas, en virtud de que el tratamiento responda a los principios previstos para la garantía del derecho a la protección de datos. Como advierte la CCE:

[176] Ortega Giménez, "La desprotección internacional del titular del de derecho a la protección de datos de carácter personal", 39.
[177] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 32.

> No podemos permitir que la negligencia o dolo de los servidores públicos llamados a desempeñar su trabajo con eficiencia y responsabilidad lesione gravemente derechos fundamentales de las personas (…) es obligación de las entidades públicas o privadas que se encargan de la recolección, manejo, archivo y circulación de información en documentos, informes, datos genéticos, bancos o archivos de datos, garantizar a las personas que la información que se recoja sea actualizada en forma permanente[178].

Desde esta perspectiva, "todo tratamiento de datos personales debe respetar todos los principios y todos los derechos, en una palabra, todo el ordenamiento jurídico de protección de datos"[179]. Sin duda, este criterio supone un presupuesto necesario para la garantía de la seguridad jurídica y confianza ciudadana en el marco de la legislación de protección de datos. Reconociendo que la falta de seguridad jurídica, no solamente podría originarse por la ausencia de aspectos legales vinculados con el tratamiento de la información. La inseguridad jurídica también es consecuencia de aspectos administrativos o prácticas de la Administración Pública que "reduzcan la confianza pública en las instituciones (judiciales, legislativas o ejecutivas) o en el goce de los derechos u obligaciones reconocidos a través de aquellas, e impliquen inestabilidad respecto del ejercicio de los derechos fundamentales, y de situaciones jurídicas en general"[180].

Ahora bien, el PLODP 2016 definió el tratamiento de datos personales como "cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal o utilizarlos en cualquier otra forma" –art. 4.10–. En este mismo orden, el art. 5.23 del PLODP 2019 introdujo en la LOPD este concepto, considerándolo como "cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado", las cuales están relacionadas con "la recogida, recopilación, obtención, registro,

[178] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –CASO Nro. 14-9-EP– publicada en el Registro Oficial Nro. 18 de 3 de septiembre de 2009.
[179] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 466.
[180] Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-24/17 relativa a la identidad de género, e igualdad y no discriminación a parejas del mismo sexo, solicitada por la República de Costa Rica, 2017.

organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales" –art. 4–[181].

En este marco, entendemos que la LOPD ha adoptado la definición del RGPD, por cuanto éste lo define como "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" –art. 4.2–. Si bien en la era digital, se destaca la importancia del tratamiento de los datos, a partir de procedimientos automatizados; advertimos que los tratamientos no automatizados o ficheros manuales siguen siendo frecuentes y su definición presenta cierta complejidad[182]. Así, precisamos que, para que una información en papel que contiene datos de carácter personal pueda ser objeto de tratamiento no automatizado o manual:

> Es necesario que esa información en papel esté contenida o destinada a ser incluida en un fichero, siendo fichero un conjunto estructurado de datos personales cuando la documentación *está organizada conforme a criterios específicos relativos a las personas que faciliten el acceso de forma sencilla a los datos* (…) como sería, por ejemplo, un fichero de historias clínicas alfabetizado por los apellidos u ordenado en virtud del DNI o del número de paciente, porque se trata de criterios específicos relativos a personas que organizan la información, permitiendo una accesibilidad sencilla y rápida[183].

[181] Sobre esta definición, la LOPD 15/1999 consideraba el tratamiento como "operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias" –art. 3. c)–.

[182] El RGPD destaca que "a fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él" –Considerando 15–.

[183] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 202.

Bajo estas consideraciones, entendemos que el proceso que concierne al tratamiento de la información debe ajustarse a procedimientos, que respeten de manera integral el ordenamiento jurídico y principios relativos a la protección de datos[184]; por cuanto "es la existencia de un tratamiento lo que hace que se dé el objeto del derecho fundamental a la protección de datos personales"[185]. En todo caso, "es necesaria, pues, cierta coordinación en el ámbito mundial en materia transferencia internacional de datos personales, con el fin último de garantizar la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos"[186].

### 2.3.11 Usuario de datos

En términos generales el usuario de datos vendría a ser la persona natural o jurídica que –distinto del titular de los datos, responsable, encargado y/o tercero–, realiza un tratamiento. El PLODP 2016 determinó que el usuario de datos era la "persona natural o jurídica, pública o privada, que realiza el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos" –art. 4.11–[187].

---

[184] El tratamiento de datos debe ajustarse al respeto y garantía del marco integral para la tutela del derecho fundamental a la protección de datos. El principio de licitud, sobre los propósitos legítimos y justos para el tratamiento de la información es trascendental en este caso. Como señala la Guía Legislativa de la OEA, el requisito de legalidad del fin para el cual se recopilan, retienen y procesan datos personales "es una norma fundamental, profundamente arraigada en valores democráticos básicos y en el estado de derecho. En principio, la recopilación de datos personales debe ser limitada y realizarse con el conocimiento o el consentimiento de la persona. No deben recopilarse datos sobre personas excepto en las situaciones y con los métodos permitidos o autorizados por Ley y (por lo general) deben darse a conocer a las personas afectadas en el momento en que se recopilen". Así también se considera que "los datos personales se recopilan por medios justos y legales cuando la recopilación es compatible tanto con los requisitos jurídicos pertinentes como con las expectativas razonables de las personas basadas en su relación con el controlador de datos o con otra entidad que recopile los datos y en el aviso o los avisos dados a las personas en el momento en que se recopilen sus datos".

[185] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 417.

[186] Ortega Giménez, "La desprotección internacional del titular del de derecho a la protección de datos de carácter personal", 43.

[187] Sobre este concepto, que no se encuentra definido como tal en el RGPD, llamaba la atención la similitud del texto que se proponía en Ecuador, con los textos que regulan la protección de datos personales en Argentina y Uruguay. Por ejemplo, la Ley Nro. 25.326 de Argentina define al "usuario de datos" como "toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos" –art.

Siendo una definición casi, textualmente, extraída de la legislación de Argentina y Uruguay; en el PLODP 2016, bien pudo confundirse con la figura del responsable, encargado, tercero y/o destinatario, dentro del tratamiento de la información, por cuanto refiere, en general, a la persona natural o jurídica que realiza un tratamiento de datos[188]. De la revisión de los textos de los países que se anotan, el usuario de datos viene a ser la persona natural o jurídica que realiza dicho tratamiento, pero que lo hace a su "arbitrio". En todo caso, tomando en cuenta que el PLODP 2016 definía que el usuario podía realizar el tratamiento, a través de conexión; apreciamos que esta definición estuvo pensada para la persona física que accede a los datos y lleva a cabo el tratamiento, dentro del ámbito del responsable o del encargado del tratamiento.

2–; y la Ley Nro. 18331 de Uruguay lo determina como "toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos" –art. 4–.

[188] Debe advertirse que, en el caso de Uruguay, según el art. 4, el usuario de datos es un concepto que se define por separado, respecto al titular de los datos, responsable, encargado, tercero y/o destinatario.

## CAPÍTULO V: LOS PRINCIPIOS Y DERECHOS DE LA PROTECCIÓN DE DATOS, COMO GARANTÍAS DEL TRATAMIENTO DE LA INFORMACIÓN PERSONAL

### 1. Introducción

El reconocimiento de principios que desarrollen la tutela del derecho fundamental a la protección de datos, es esencial por cuanto garantizan que el tratamiento de la información personal cumpla con el respeto de los derechos y libertades de las personas[1]. Esto se traduce, "en la obligación de las empresas a la hora de revisar y hacer guardar estos principios siempre que apliquen técnicas de privacidad desde el diseño a nuevos tratamientos, pues deberán comprobar que los mismos cumplen con unas condiciones mínimas de garantía para los derechos de los afectados"[2]. Los principios, se afirman en un conjunto de normas y condiciones que "determinan cómo se deben recoger, tratar y ceder los datos de carácter personal, a los efectos de garantizar la intimidad y demás derechos fundamentales de los titulares de los datos, los consumidores o usuarios, y en definitiva, los ciudadanos"[3].

La incorporación de este conjunto de normas y condiciones en la legislación; pretenden interpretar su significado de manera global y que, interrelacionados entre sí, articulen un sistema integral, equilibrado y eficaz para la seguridad jurídica que debe ofrecer este derecho fundamental. En otras palabras, "la cuestión estriba entonces en determinar cuál es el contenido esencial de tal derecho; los principios y características que lo definen y que no pueden ser desconocidos so pena de desconocer y en consecuencia violentar el propio derecho"[4]. Así, por una parte, los

[1] Como señala el RGPD, "los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal –Considerando 2–.

[2] Joaquín Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 347.

[3] Javier Puyol Montero, "Los principios del Derecho a la Protección de Datos", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 135.

[4] Pablo Lucas Murillo de la Cueva y José Luis Piñar Mañas, El *derecho a la autodeterminación informativa* (Madrid-México: Fontamara S.A, 2011), 101.

principios constituyen “las obligaciones que incumben a los responsables del tratamiento y que deben estructurar todos los tratamientos de datos personales. Por otra parte, estos principios también pueden ser comprendidos como derechos de las personas cuyos datos sean objeto de tratamiento”[5]. En todo caso, subrayamos que los responsables del tratamiento “han de integrar de un modo natural en sus procesos para que sirvan de punto de partida en lo que respecta al cumplimiento normativo en materia de protección de datos”[6]. Por ello, frente al tratamiento de la información, su observancia “garantiza una utilización racional y razonable de los datos personales, que permite compatibilizar el desarrollo informático y las necesidades sociales con el respeto más escrupuloso a los derechos y libertades de las personas”[7].

Tomando en cuenta que la CCE, caracteriza el derecho a la protección de datos como un derecho complejo que comprende algunas dimensiones relacionadas con el tratamiento de la información personal[8]; es necesario esclarecer estos supuestos, a partir del análisis de los principios generales, por cuanto “tienen naturaleza normativa y van a informar e integrar la interpretación de toda esta normativa (…) supliendo directamente las múltiples lagunas legales que se puedan producir en la propia regulación, a consecuencia de la imparable evolución de la tecnología”[9]. Por ejemplo, considerando que la efectividad de estos principios, “requieren el reconocimiento, garantía y tutela de los derechos de acceso, rectificación, cancelación y oposición”[10]. En esta parte, será de gran utilidad la jurisprudencia de la CCE. Entre otras, la sentencia 19-9-SEP-CC, facilitará el estudio del contenido y

[5] Antonio Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, (Valencia: Tirant lo Blanch, 2010), 394.
[6] Muñoz Ontier, “Disposiciones Generales (Arts. 1-5)”, 347.
[7] Ana Isabel Herrán, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, (Madrid: Dykinson, 2002), 210.
[8] Sobre esta reflexión, la CCE agrega que “dicho criterio está expresado en la doctrina por el criterio de Oscar Puccinelli, quien señala lo siguiente: [P]or derecho a la protección de datos se propone entender la suma de principios, derechos y garantías establecidos en favor de las personas que pudieran verse perjudicadas por el tratamiento de los datos nominativos a ella referidos". Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 67-11-JD– publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.
[9] Puyol Montero, “Los principios del Derecho a la Protección de Datos”, 135.
[10] Lucas Murillo de la Cueva y Piñar Mañas, El *derecho a la autodeterminación informativa*, 102.

desarrollo de cada principio que se encuentra vinculado al derecho a la protección de datos[11]. De esta manera, los principios que engloba el tratamiento de la información de carácter personal se abordarán conforme a la nueva normativa de protección de datos –en adelante LOPD–, que fue aprobada en mayo de 2021 y, además, tomando como referencia los proyectos de Ley en Ecuador. Lógicamente, la doctrina, el RGPD, los EPEI y la Guía Legislativa de la OEA permitirán establecer si dichos principios corresponden a una regulación, que garantice la integridad y coherencia del marco jurídico de protección que se propone[12].

### 1.1 El principio de licitud

La CCE define el principio de licitud como uno de los fundamentos del derecho a la seguridad jurídica, por cuanto garantiza el respeto del orden constitucional y de las normas jurídicas que deben ser aplicadas por las autoridades competentes. Constituye un supuesto que pretende asegurar la confianza ciudadana y la legitimidad del ordenamiento jurídico, en el marco de la protección de la información de carácter personal. Así, como destaca la CCE, la seguridad jurídica constituye:

> El pilar sobre el cual se asienta la confianza ciudadana en cuanto a las actuaciones de los distintos poderes públicos; en virtud de aquello, los actos emanados de dichas autoridades públicas deben contener un apego a los preceptos constitucionales, reconociendo la existencia de las normas que integran el ordenamiento jurídico ecuatoriano, las mismas que deben ser claras y precisas, sujetándose a las atribuciones que le compete a cada órgano[13].

[11] Así, como la Sentencia 1-14-PJ0-CC de la CCE es de análisis obligatorio para contextualizar el contenido del derecho a la protección de datos personales; la Sentencia 19-9-SEP-CC es esencial para definir el contenido y la finalidad del *habeas data*. Dicha sentencia afirma que el *habeas data,* constituye una garantía que "tiene como finalidad el acceso a los documentos, bancos o archivos referentes a la persona solicitante que consten en entidades públicas o privadas, así como en caso de que la información proporcionada resulte falsa, errónea, antigua, incierta, obsoleta, discriminatoria o inexacta, exigir su actualización, rectificación, eliminación, anulación o confidencialidad".

[12] Tomando en cuenta que la normativa de protección de protección de datos tiene por objeto también establecer normas relativas a la libre circulación de los datos personales, el RGPD agrega que la normativa debe "contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas" –Considerando 2–.

[13] Véase la Resolución de la Corte Constitucional 182, Sentencia Nro. 182-15-SEP-CC –CASO Nro. 1493-10-EP– publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015.

Tanto en el ámbito público como privado, el tratamiento de la información debe enmarcarse en la aplicación de la normativa que reconoce y garantiza el derecho a la protección de datos. En este sentido, los principios para la protección de los datos "constituyen el contenido esencial del derecho a la protección de datos, y que a través de los mismos, se configura un sistema de tutela que garantiza una utilización más racional y razonable de los datos personales"[14]. Por tanto, en el tratamiento de datos, mediante el cumplimiento de una obligación legal o, en virtud, del interés público o ejercicio de la Administración:

> Habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al usuario en ese proceso y, en particular, las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista[15].

En este marco, el principio de licitud está orientado a garantizar que los datos personales sean tratados de manera lícita y, por ende, sean recopilados para fines legítimos y por medios justos y legales. Por tanto, "la legitimidad de la finalidad es lo que justifica que se puedan recoger y tratar datos personales. Una finalidad, para que sea considera legítima, debe estar ajustada a la Constitución y a la Ley"[16]. En consecuencia, "los datos alcanzan determinada calidad y es lícito su tratamiento porque son puestos en relación con los fines legítimos que inspiran el tratamiento"[17].

Según el PLODP 2016, este principio suponía que, la formación de bases de datos o recopilación de la información era lícita, "cuando se encuentren debidamente inscritas y la información haya sido obtenida por medios legítimos en estricta observancia a la normativa en el ámbito relativo a esta materia" –art. 3.1–. Aunque, la recogida de la información personal debe efectuarse en estricta observancia de la normativa de protección de datos, también se hacía referencia a la licitud de la formación de bases de datos, siempre y cuando se encontraran, debidamente, inscritas. En este punto, señalamos que la obligación de inscripción de las bases de

[14] Puyol Montero, "Los principios del Derecho a la Protección de Datos", 136.

[15] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 348.

[16] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 396.

[17] Herrán, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, 211.

datos desaparece en modelos de regulación comparados, como así lo establece el RGPD. Así, la importancia de este principio no radica en la inscripción de las bases de datos. Lo esencial es prever que la información personal sea recabada u obtenida por medios legítimos, atendiendo los principios que comporta la protección integral de este derecho.

Como advertimos, “no es suficiente que el fin sea legítimo, que ha de serlo, sino que además se exige que los fines sean explícitos y se encuentren determinados porque sólo así puede garantizarse la eficacia y virtualidad de la calidad de los datos”[18]. Por ello, se precisa garantizar que la recopilación, almacenamiento y utilización, no sean arbitrarias y desproporcionadas, en relación a la finalidad para la cual fueron recabados los datos personales[19]. De esta manera, subyace el principio de limitación de la finalidad, por el cual “se exige que los datos sean recogidos siempre asegurando fines determinados, explícitos y legítimos, y garantizando que no serán tratados ulteriormente de manera incompatible con dichos fines”[20].

Sobre este principio, el RGPD señala que los datos personales serán "tratados de manera lícita, leal y transparente en relación con el interesado” –art. 5.1. a)–. Siguiendo las previsiones señaladas por el RGPD, el PLODP 2019 coincidió en reconocer que “en ningún caso los datos personales podrán ser tratados a través de medios o para fines ilícitos o desleales” y que, por tanto, “las relaciones derivadas del tratamiento de datos personales deben ser transparentes” –art. 9–. En este marco, por una parte, la LOPD reconoce que, mediante el principio de juridicidad “los datos personales deben tratarse con estricto apego y cumplimiento a los

[18] Ibíd., 212.
[19] Sobre este principio, la Guía Legislativa de la OEA señala que: “Los datos personales deben ser recopilados solamente para fines legítimos y por medios justos y legales. Este principio abarca dos elementos: 1) los “fines legítimos” para los cuales se recopilan inicialmente los datos personales y 2) los “medios justos y legales” con los cuales se efectúa la recopilación inicial. La premisa es que muchas o incluso la mayoría de las intrusiones en los derechos de las personas pueden evitarse si se respetan los conceptos conexos de legalidad y justicia desde el comienzo, cuando se recopilan inicialmente los datos. Desde luego, estos principios se aplican y deben respetarse en todo el proceso de recopilación, compilación, almacenamiento, utilización, divulgación y eliminación de datos personales, no solo en el momento de su recopilación. Sin embargo, es más probable que se cumplan y se respeten si se recalcan y se respetan desde el comienzo”.
[20] Muñoz Ontier, “Disposiciones Generales (Arts. 1-5)”, 349.

principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la presente Ley, su Reglamento y la demás normativa y jurisprudencia aplicable" –art. 10. a)–; y, por otra que, a través de la lealtad, en el tratamiento de datos "debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados" y, por tanto "en ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales" –art. 10. b)–. De este modo, entendemos que se obliga a que el responsable sea transparente "con la información acerca de sus intenciones de tratamiento de datos del usuario y no debe ocultar al mismo ninguna finalidad con la que vaya a tratar su información, por obvia que esta parezca o por mucho que fuere una práctica habitual"[21].

Es de este modo que, el RGPD introduce, conjuntamente, con el principio transparencia, el principio de licitud del tratamiento, el cual "viene fundamentado por la necesidad de que el titular del dato, el ciudadano, no se vea desprotegido ante eventuales tratamientos que desconoce o que se están realizando de forma ilícita"[22]. En este orden, también destacamos que el PLODP 2019 buscó proteger al titular de los datos, frente al tratamiento ilícito, mediante el principio de legitimidad, por lo que, a continuación, señalaremos algunas similitudes y diferencias entre el RGPD, el PLODP 2019 y la actual LOPD, en cuanto a las condiciones que se prescriben para que el tratamiento sea lícito.

Entre las semejanzas, por ejemplo, indicamos que el RGPD determina que el tratamiento es lícito cuando interesado haya entregado su consentimiento "para el tratamiento de sus datos personales para uno o varios fines específicos" –art. 6.1. a)–; mientras que el PLODP 2019 expuso que sería válido cuando el titular haya entregado dicho consentimiento "para el tratamiento de sus datos personales para una o varias finalidades específicas" –art. 10.6–. Esta prescripción ha sido adoptada

[21] Ibíd., 348.

[22] Natalia Martos, "Principios (Arts. 6-11)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 353.

por el legislador en el art. 7.1 de la LOPD. Además, el RGPD habilita el tratamiento cuando "es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento" –art. 6.1. c)–; en tanto que el PLODP 2019 prescribió que procedía cuando existiera: "una obligación en el ordenamiento jurídico aplicable al responsable del tratamiento" –art. 10.1– y que, en todo caso, se desprendiera de una "orden judicial, resolución o mandato motivado de autoridad pública competente" –art. 10.2–. Dichas disposiciones, respectivamente, han sido ratificadas por la LOPD, tanto el art. 7.2 como en el art. 7.3. Por último, el RGPD legitima el tratamiento cuando éste "es necesario para proteger intereses vitales del interesado o de otra persona física" –art. 6.1. d)–; en tanto que el PLODP 2019 advirtió que, en el mismo sentido, dicha legitimación se concretaría para "proteger intereses vitales del interesado o de otra persona natural, como por ejemplo su vida, salud o integridad" –art. 10.7–[23]. Naturalmente, se trata de una condición que también ha sido aprobada por el legislador en la LOPD, al tenor del art. 7.6.

Ahora bien, encontramos algunas diferencias cuando el RGPD señala el caso de que el tratamiento será licito por "la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales" –art. 6.1. b)–. Al respecto, el PLODP 2019 confundió este supuesto, señalando que procedía, en virtud del cumplimiento de "obligaciones contractuales perseguidas por el responsable del tratamiento, encargado o un tercero legalmente habilitado" –art.

[23] La única diferencia significativa, en esta parte, es que la LOPD señala que la legitimación del tratamiento se hará para proteger los intereses vitales del "interesado", cuando a lo largo de sus disposiciones conceptualiza a éste como el titular de datos personales. Naturalmente, producto de la reproducción de las disposiciones del RGPD, entendemos que no altera el sentido de este supuesto de legitimación. No obstante, frente a esta distinción, consideramos necesario aclarar que, "en la versión en inglés del RGPD se habla de «sujeto o titular» de los datos («*data subject*») y en la versión en francés, de «persona concernida» («*personne concernée*»). Y creemos que cualquiera de estas dos denominaciones es mejor que la escogida en la versión española, porque no es lo mismo ser el titular, el concernido o el afectado por los datos, que el interesado en los datos. Interesados hay muchos. El término «interesado» va a suscitar problemas de interpretación y de aplicación del RGPD, pues se pone al titular, concernido o afectado por los datos al mismo nivel que una empresa o administración, que pueden alegar un «interés legítimo» o «público», respectivamente, para utilizar datos personales sin necesidad del consentimiento del titular, concernido o afectado". Cfr. Borja Adsuara Varela, "El ciudadano frente al Reglamento", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 168.

10.4–. En todo caso, la LOPD ha subsanado este aspecto, considerando la licitud por “la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado” –art. 7.5–

Además, si bien el RGPD determina la licitud cuando “el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño” –art. 6.1. f)–; el PLODP 2019 también confundió este supuesto, apuntando que procedía el tratamiento cuando resultara de “la ejecución de medidas precontractuales a petición del titular, excepto cuando prevalezcan los intereses o los derechos y libertades de niñas, niños y adolescentes como titulares” –art. 10.5–. Naturalmente, siguiendo la normativa del RGPD, el legislador ha aclarado en la LOPD que esta condición implica “satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma” –art. 7.8–.

Al parecer, parte del contenido del art. 10.5 del PLODP 2019 que refería a la legitimación en “la ejecución de medidas precontractuales a petición del titular” debía formar parte del supuesto planteado en el art. 10.4, con el objeto de guardar correspondencia con el art. 6.1. b) del RGPD. De la misma manera, cuando el art. 10.4 del PLODP 2019 determinaba la legitimación en el cumplimiento de “obligaciones contractuales”, este supuesto debía formar parte del art. 10.5, a fin de establecer una regulación semejante a la dispuesta en el art. 6.1. f) del RGPD. En todo caso, el art. 10.5 del PLODP 2019 omitió señalar que dicha legitimación se haría cuando fuera necesario para la satisfacción de intereses legítimos, lo cual significaba que el responsable debía “realizar una ponderación meticulosa para garantizar que goza de una base jurídica para el tratamiento que no prevalezca

sobre los intereses o derechos y libertades del sujeto titular del dato"[24]. Con referencia a este aspecto, anotamos que el responsable del tratamiento debe valorar:

> El interés que ostenta desde una perspectiva abstracta, para comprobar que, efectivamente, dicho interés no infringe ninguna norma o derecho de terceros y, por tanto, es legítimo. En segundo lugar, también desde una perspectiva abstracta, el responsable tendrá que ponderar el interés que persigue y la incidencia que el tratamiento de datos que se propone tendrá sobre los derechos fundamentales y los simples derechos de los interesados, a fin de determinar si esa incidencia hipotética tiene una relevancia equilibrada frente al interés que persigue, o no. Si la comparación entre el interés y la vulneración que provoca sobre los intereses afectados conduce a la conclusión de que no existe un desequilibrio en perjuicio de los intereses afectados, el responsable podrá iniciar el tratamiento tras haber informado de ello a los interesados, identificando el interés legítimo que invoca[25].

Finalmente, otra condición que plantea el RGPD es cuando el tratamiento sea "necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento" –art. 6.1. e)–. Si bien el PLODP 2019 precisó que el tratamiento sería legítimo por "el ejercicio de competencias y facultades establecidas en la Constitución, la Ley e instrumentos internacionales aplicables a las entidades del sector público" –art. 10.3–; en este punto, la propuesta no determinó que, como una condición de licitud, el tratamiento se realizaría por el cumplimiento de una misión realizada en interés público. En todo caso, la LOPD ha dispuesto que, finalmente, esta condición se manifiesta cuando el tratamiento "se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley"; todo ello, "sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad" –art. 7.4–. Desde esta perspectiva, el tratamiento basado en el interés público subraya que "se debe tener en cuenta, entre otras

[24] Martos, "Principios (Arts. 6-11)", 354.

[25] Aparicio Salom, "Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23)", 411. En todo caso, advertimos que "si es preocupante la equiparación de las condiciones para la licitud de los datos, en el caso del «interés público» de las administraciones, mucho más preocupante lo es en el caso del «interés legítimo» de las empresas, por el que éstas pueden realizar un tratamiento de datos personales sin consentimiento de los titulares (o afectados). Habiendo desaparecido el límite de las «fuentes accesibles al público»". Cfr. Adsuara Varela, "El ciudadano frente al Reglamento", 170.

cosas, cualquier relación entre los fines que justificaron la recogida de los datos y los fines del tratamiento previsto posteriormente"[26].

En este ámbito, la LOPDGDD dispone que el tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos se considerará lícito cuando esté "fundado en el cumplimiento de una obligación legal exigible al responsable –art. 8.1–; y que, además, "solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de Ley –art. 8.2–[27].

Así también los EPEI, frente al principio de licitud, precisan que los responsables y autoridades públicas deberán tratar los datos personales "con estricto apego y cumplimiento de lo dispuesto por el derecho interno del Estado Iberoamericano que resulte aplicable, el derecho internacional y los derechos y libertades de las personas" –art. 14.1–. Esta sería una importante prescripción que desarrolle el principio de licitud, por cuanto a la luz del art. 7.4 de la LOPD, en el marco del Estado constitucional de derechos y justicia, el principio de eficacia directa implica, no solamente la aplicación directa e inmediata de los derechos y garantías reconocidos en la Constitución sino, además, de los derechos y libertades establecidos en los instrumentos internacionales.

Como se sabe, "la legislación de protección de datos personales recoge un conjunto de garantías para los ciudadanos y establece los criterios para hacer compatibles todos los derechos fundamentales en presencia"[28]. Por ello, es importante que el

[26] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 348.

[27] Hay que recordar que la LOPD 15/1999 enmarcaba al principio de licitud en el principio general de "calidad de datos" señalando que los datos personales podían ser recogidos y sometidos a tratamiento "cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido" –art. 4.1–. Así también prohibía "la recogida de datos por medios fraudulentos, desleales o ilícitos" –art. 4.7–. En todo caso, en lo que refiere a la situación de España, hay que señalar que "no se desarrolló, sino hasta muy tarde, la aplicación del interés legítimo como causa habilitante para el tratamiento de datos personales, pero se permitió el sistema que se denominó consentimiento tácito". Cfr. Aparicio Salom, "Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23)", 411.

[28] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 396.

tratamiento de la información, –desde el momento en que inicia, es decir, a partir de que ha sido ha sido recabada–, se cumpla, a través de medios legítimos y legales contemplados en la legislación. Sin embargo, como hemos planteado, cuando el responsable del tratamiento "no tenga cobertura exacta en ninguno de esos supuestos, no se excluye necesariamente la licitud del tratamiento, siempre y cuando realice una ponderación que es legalmente exigible ya que, fuera de dichos supuestos, el responsable no goza de la presunción «*iuris tantum*» de prevalencia del interés legítimo"[29].

Por último, en relación a los principios de lealtad y transparencia, advertimos una significativa conexión con el principio de licitud. Así, por una parte, "se establece que el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial"[30]. Y por otra, se desarrolla un concepto clave, en relación a las condiciones para que el tratamiento se considere lícito. Es decir, el de la expectativa razonable de privacidad del titular, por el cual, "el responsable debe considerar cuál es la intención del interesado al entregarle sus datos, qué espera recibir en contraprestación y cuál es el uso máximo que entiende razonable por parte del responsable a cambio de sus datos"[31].

De esta manera, para que el tratamiento sea lícito, debe privilegiarse los derechos de los titulares de los datos personales, garantizando el derecho a conocer los fines y características del tratamiento. Incluso, como dispone, tanto el RGPD como los EPEI, el principio de licitud, no solamente garantiza la recopilación inicial de los datos personales. Este principio se aplica de manera integral en todo el tratamiento de la información, de tal suerte que, todo tratamiento contrario al principio de calidad

[29] Martos, "Principios (Arts. 6-11)", 353.
[30] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 348.
[31] Ibíd.

de datos, lealtad y transparencia puede derivar en una ilicitud, que afecta el derecho a la protección de datos personales en su conjunto[32].

En nuestro concepto, siguiendo el ejemplo del RGPD; el PLOPD 2019 presentó disposiciones más completas sobre el principio de licitud, señalando las condiciones para que el tratamiento de datos personales sea lícito, las cuales fueron finalmente mejoradas por el legislador en la LOPD. En el caso del PLOPD 2016, evidentemente, éste requirió una necesaria reformulación, en cuanto a la denominación de este principio, toda vez que, si bien, la propuesta hizo referencia al principio de legalidad, de conformidad al análisis expuesto su naturaleza correspondía al de licitud en el tratamiento de la información. Asimismo, considerando que la Constitución, por medio del *habeas data* garantiza el origen y destino de la información personal; el PLOPD 2016 debió, además, incorporar en su regulación los principios de lealtad y transparencia, a fin de garantizar que el tratamiento de los datos personales se revistiera de legitimidad en su conjunto; y asimismo, garantizara seguridad jurídica de la legislación de protección de datos[33].

### 1.1.1 Condiciones para el consentimiento

En el derecho a la protección de datos el consentimiento es visto como un elemento de legitimación que se aplica, tanto a los tratamientos de la información de carácter personal como a la comunicación de datos a un tercero[34]. En el marco europeo, el consentimiento "juega un papel fundamental que cambia el sistema de registro y recabo de datos en todo tipo de servicios de la sociedad de la información"[35] y, por

[32] No está por demás advertir que, cuando el titular de los datos considere que "se están usando sus datos sin su consentimiento expreso o para un fin no autorizado y que la administración o empresa no está amparada por un interés público o legítimo, lo primero que debe hacer es dirigirse al responsable de dicho tratamiento (la administración o empresa) e intentar que cese inmediatamente en dicho tratamiento". Cfr. Adsuara Varela, "El ciudadano frente al Reglamento", 172.

[33] Este es un aspecto que, si se encontraba recogido en el PLOPD 2019, por medio de los principios de juridicidad, lealtad y transparencia, los cuales estaban orientados a garantizar que "los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución" –art. 9–.

[34] Cfr. Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 462.

[35] Martos, "Principios (Arts. 6-11)", 357.

tanto, es exigido como un elemento de determinación de la legitimación o licitud de los tratamientos de datos[36]. Significa un presupuesto integrador que, en el marco de regulación del derecho a la protección de datos, pretende atribuir legitimidad e impedir efectos negativos en los derechos y libertades del titular.

Como señala la CCE, el derecho a la protección de datos faculta al titular "a decidir y consentir de forma informada y libre el uso de sus datos personales por terceros, ante el tratamiento automatizado de los mismos"[37]. Este derecho a consentir de forma informada y libre garantiza la legitimidad del tratamiento de la información personal, y, además, asegura el derecho a la información sobre los fines de dicho tratamiento. En este sentido, la Guía Legislativa de la OEA destaca que "el consentimiento de la persona debe basarse en suficiente información y debe ser claro, es decir, no debe dar lugar a ninguna duda o ambigüedad con respecto a la intención de la persona". Por ello, consideramos que, "a partir del reconocimiento de un derecho a consentir el tratamiento de los datos se estructura y organiza la autodeterminación informativa o la facultad de los interesados de establecer y decidir sobre el tratamiento de la información que les concierne"[38].

Como un elemento de legitimación de los tratamientos, el incumplimiento de las condiciones de licitud, a partir del consentimiento, constituye un abuso e intromisión en los derechos y libertades que se vinculan con el tratamiento de la información que –salvo las excepciones que al final se anotarán–, deslegitima en su contexto, más amplio, el procesamiento y divulgación de los datos. De esta manera, el respeto del derecho a la protección de datos implica la garantía de un conjunto de derechos y obligaciones, en donde, el consentimiento del interesado, "no es el único principio ni la única facultad que conforma el contenido esencial de este derecho

[36] En este aspecto, la Guía Legislativa de la OEA señala que "la recopilación de datos personales debe ser limitada y realizarse con el conocimiento y consentimiento de la persona (…) La recopilación y el procesamiento de datos de acuerdo con la condición de los intereses legítimos deben ser justos y legales y ceñirse a todos los principios de la protección de datos".
[37] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 67-11-JD– publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.
[38] Herrán, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, 220.

fundamental[39]. Como hemos señalado, el respeto de este derecho comporta la garantía de principios esenciales como el de calidad de datos. Por ello, a partir del consentimiento, deben respetarse otros deberes como el de informar y adoptar mecanismos lícitos –libres de engaño, intimidación, coacción o consecuencias negativas–, para obtener la autorización del tratamiento.

En este marco, al igual que el art. 7.1 de la LOPD, el RGPD precisa como una condición de licitud del tratamiento que el interesado haya entregado su consentimiento "para el tratamiento de sus datos personales para uno o varios fines específicos" –art. 6.1. a)–. Aquí, la novedad que introduce esta normativa no se encuentra en el consentimiento como supuesto de legitimación, sino en la forma en la que debe entenderse que éste es prestado: bien, a través de una declaración o una clara acción afirmativa. Precisamente, este sí es un vacío que deberá subsanarse en la formulación del reglamento de la LOPD. Recordemos que estas especificaciones las encontramos en el art. 4.11 del RGPD, en donde se señala que el consentimiento es "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". De este modo, "si hay consentimiento (libre, informado, expreso y específico), puede hacerse —casi— cualquier cosa, o tratamiento. Pero, si no hay consentimiento, no puede ni tocarse a una persona, ni tratar un dato"[40].

Siendo el consentimiento uno de los fundamentos jurídicos del tratamiento lícito de los datos personales, el RGPD advierte algunas condiciones para que este consentimiento pueda considerarse válido. Así, para que el consentimiento prestado por el interesado sea considerado legítimo, "el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales" –art. 7.1–; en el contexto de una declaración escrita, "que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje

[39] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 466.
[40] Adsuara Varela, "El ciudadano frente al Reglamento", 169.

claro y sencillo" –art. 7.2–; debe garantizarse que el interesado tenga "derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo". –art. 7.3–; y "al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato" –art. 7.4–.

Siguiendo la línea del RGPD, la LOPDGDD, sobre el tratamiento basado en el consentimiento del afectado, determina su legitimación "cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas" –art. 6.2–. Así también "no podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual" –art. 6.3–[41].

Ahora bien, los EPEI refieren dos condiciones. Primero, "cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara" –art. 12.1–. Y segundo, "siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos" –art. 12.2–. De las disposiciones que se anotan, entendemos que –en la recopilación o recogida de datos

[41] Recordemos que la LOPD 15/1999 enmarcaba al consentimiento como un principio del derecho a la protección de datos. Al respecto, esta Ley consideraba que "el titular de los datos deberá prestar su consentimiento libre, expreso, previo e informado para la entrega de los mismos. Se exceptúan los datos que provengan de fuentes públicas de información; se recaben para el ejercicio de funciones propias de las instituciones del Estado; deriven de relaciones contractuales, científicas o profesionales del titular de los datos y sean necesarias para su cumplimiento; y se realicen por personas naturales para su uso exclusivo personal o doméstico" –art. 3.4–.

personales– el consentimiento coexiste con el principio de transparencia e información, a partir de, la excepcionalidad que plantea el tratamiento de la información que provenga de fuentes públicas y se recaben dentro del marco de prácticas o políticas que en las entidades públicas consideren como necesarias para el ejercicio de sus funciones propias[42]. De esta manera, subrayamos que la transparencia e información al interesado impide que los tratamientos de datos "se puedan hacer «a espaldas» de las personas titulares de los datos. En efecto, por un lado, cualquier tratamiento debe ser declarado previamente y no se puede realizar sin que se tenga un conocimiento público de él"[43]. Por esta razón, "hay que estar a lo que dicta el principio de transparencia, esto es, que la información dirigida al público sea concisa, fácilmente accesible, fácilmente entendible y que se utilice en un lenguaje claro"[44].

En consecuencia, primero, advertimos que:

> Le corresponde al responsable del tratamiento la carga de la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho (…) En segundo lugar, el consentimiento debe ser libre, de manera que el consentimiento no es una base jurídica válida cuando existe un desequilibrio entre el interesado y el responsable del tratamiento. Así, se establecen unas condiciones que garanticen que el consentimiento es libre y específico. En tercer lugar, el consentimiento debe ser específico, por lo que el RGPD trata de que el consentimiento para el tratamiento de datos personales se distinga de cualquier otra dación de consentimiento para otro asunto[45].

Tomando en cuenta que, en el caso de la Administración Pública, el respeto del consentimiento, implica ponderar un interés público, es importante que las administraciones asuman, responsablemente, la garantía de los principios que

---

[42] Sobre esta relación, la Guía Legislativa de la OEA precisa que "este principio también se centra en la recopilación de datos personales. Se basa en el concepto de la "autodeterminación en lo que respecta a la información" y, en particular, en dos conceptos que gozan de amplio reconocimiento a nivel internacional: el principio de "transparencia" y el principio de "consentimiento". Combinados, estos principios requieren que 1) se especifiquen los fines para los cuales se recopilen datos personales, generalmente a más tardar en el momento en el cual se inicie la recopilación; y 2) se recopilen datos personales solo con el consentimiento (explícito o implícito) de la persona a la que se refieran".

[43] Ramon Oró, *La protección de datos*, (Barcelona: Oberta UOC, 2015), 64

[44] Martos, "Principios (Arts. 6-11)", 358.

[45] Antonio Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada*, Nro. 49 (2018), 187-266.

comprende el derecho a la protección de datos, por cuanto como refiere la CCE "corresponde también un manejo responsable de la misma, debido a que cualquier acción u omisión en su tratamiento por parte de los servidores públicos responsables puede generar una violación a derechos fundamentales de las personas"[46]. Debido a la importancia que tiene garantizar que el consentimiento sea prestado de manera informada y exento de medios ilícitos, es esencial la función que cumplen los responsables del tratamiento para el desarrollo y ejercicio de este supuesto. Si bien, en materia de derechos y garantías constitucionales, a la Administración Pública le corresponde interpretarlos en el sentido que más favorezca su efectiva vigencia. Posibles escenarios que manifiesten la oscuridad de la normativa prevista en la LOPD no pueden invocarse para justificar las violaciones en que incurran los responsables, en cuanto al respeto de los principios o supuestos de legitimación que comporta la garantía de este derecho fundamental[47].

Bajo estas consideraciones, las previsiones sobre el consentimiento se consideraban insuficientes en el PLODP 2016. Tan solo el PLODP 2019 hizo referencia a algunos supuestos para la validez del consentimiento, enfatizando en que éste debía entregarse, expresamente, de manera que "el responsable pueda demostrar que el titular manifestó su voluntad a través de una declaración o acción clara, afirmativa o se deduzca de una acción del titular" –art. 14–. En todo caso, ambos proyectos coincidieron en que el consentimiento podría revocarse. Así, el PLODP 2016 reconoció como un derecho del titular de los datos personales la facultad de "revocar el consentimiento" –art. 6.5–; y el PLODP 2019, como parte del principio del consentimiento, estableció que "en cualquier momento, sin que sea

[46] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –CASO Nro. 14-9-EP– publicada en el Registro Oficial Nro. 18 de 3 de septiembre de 2009.

[47] Así, conforme el derecho fundamental que se encuentra reconocido en el art. 66.19 de la Constitución de Ecuador, la administración no debe tener reparos en considerar que "la recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley*";* y así también estimar que, conforme a la garantía constitucional del art. 92, respecto al *habeas data,* "las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la Ley".

necesaria una justificación (…) el tratamiento realizado antes de revocar el consentimiento es lícito" –art. 14–[48].

Además, si bien estas propuestas legales coincidieron con la normativa europea, en cuanto a caracterizar que el consentimiento debe derivarse de forma libre, específica (expresa), informada (previa e informada); el PLODP 2016 se alejó de la regulación española y comunitaria en relación a que el consentimiento debía ser inequívoco, es decir que no admita duda, equivocación o pueda resultar de una suerte de presunción del consentimiento[49]. Sobre este respecto, subrayamos que, en el RGPD se trata de una modificación importante al introducir "«inequívoco» (*unambiguous*) como uno de los requisitos de la «indicación de los deseos del sujeto de los datos» (o de la «manifestación de voluntad del interesado»), para que sea válido el consentimiento"[50]. Por tanto, en la interpretación del consentimiento se exige que éste indique que el titular de los datos personales "acepta la propuesta de tratamiento de sus datos personales (…) De lo que se trata es que cuando se pretenda que la base jurídica de la licitud del tratamiento sea el consentimiento, este se esté prestando realmente y que no genere dudas"[51].

[48] Si el consentimiento no ha sido obtenido, a través de mecanismos claros de información –y, en suma, por medios lícitos– es evidente la necesidad de garantizar la facultad de revocarlo, por cuanto el titular de los datos no lo ha autorizado. Por consiguiente, no existe una habilitación legal para realizar un tratamiento. Como señala la Guía Legislativa de la OEA, "una persona tiene derecho a retirar el consentimiento según la índole del consentimiento dado y los fines para los cuales se recopile la información. En general, el retiro del consentimiento no afecta la validez de lo que ya se haya hecho sobre la base del consentimiento".

[49] La Agencia Española de Protección de Datos, siguiendo los criterios sentados en las diversas recomendaciones emitidas por el Comité de Ministros del Consejo de Europa, interpreta el término "Inequívoco", manifestando que: "no resulta admisible deducir el consentimiento de los meros actos realizados por el afectado (consentimiento presunto), siendo preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento". Adicionalmente, la Guía Legislativa de la OEA caracteriza el consentimiento precisando que "por lo general, la persona debe ser capaz de dar su consentimiento libremente respecto de la recopilación de datos personales de la forma y con los fines previstos (…) Para que el consentimiento sea válido, la persona debe contar con suficiente información sobre los detalles concretos de los datos que se recopilarán, la forma en que se recopilarán, los fines del procesamiento y toda divulgación que pueda efectuarse. La persona debe ser capaz de efectuar una elección real".

[50] Borja Adsuara Varela, "El consentimiento", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 157.

[51] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 221.

En todo caso, advertimos que el PLODP 2019 determinó que el consentimiento sería válido cuando se prestara de manera inequívoca, es decir, "que no se presenten dudas sobre el alcance de la autorización otorgada por el titular" –art. 14–. Por ello, hay que reconocer que el PLODP 2019 constituyó la mejor propuesta que, acorde a los modelos internacionales expuestos, representaba un marco adecuado de garantía del derecho a la protección de datos. A diferencia del RGPD, quedaba pendiente que, tanto el PLODP 2019 distinguiera si el consentimiento se plantearía como un elemento de legitimación en los tratamientos de la información de carácter personal, ya que, como hemos evidenciado, ambas propuestas coincidieron en enmarcar al consentimiento como un principio del derecho a la protección de datos. Al final, esta distinción se ha concretado en la aprobación de la LOPD, por cuanto el legislador ha considerado pertinente señalar las condiciones por las cuales el consentimiento es válido o legítimo, por ejemplo, cuando sea "libre, es decir, cuando se encuentre exento de vicios del consentimiento" –art. 8.1–; "específico, en cuanto a la determinación concreta de los medios y fines del tratamiento" –art. 8.2–; "informado, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia" –art. 8.3–; "inequívoco, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular" –art. 8.4–.

### 1.2 El principio de pertinencia

Este principio implica una garantía de razonabilidad sobre los fines, por los cuales se lleva a cabo el tratamiento de la información personal. Es decir que el tratamiento debe ser pertinente en relación a unos fines legítimos y responder a un contexto específico, a partir de su recopilación, uso y divulgación. En este sentido, subrayamos que "la recogida de datos y su posterior tratamiento sólo es legitima si los datos son adecuados, pertinentes y no excesivos para obtener la finalidad"[52].

[52] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 398.

La Guía Legislativa de la OEA señala que en el principio de pertinencia los datos personales deben "guardar una relación razonable con los fines para los cuales hayan sido recopilados y se tenga la intención de usarlos"[53]. Así, los EPEI enmarcan este principio dentro de los principios de finalidad y proporcionalidad para el tratamiento de la información, considerando que, por un lado, el responsable "no podrá tratar los datos personales en su posesión para finalidades distintas a aquéllas que motivaron el tratamiento original de éstos" –art. 17.2– y que, además, "tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento" –art. 18.1–. De este modo, los EPEI hacen referencia al principio de minimización de datos, recogido en el RGPD, por el cual el responsable del tratamiento "procurará en todo caso recabar y utilizar la menor información posible del interesado para cumplir con las finalidades legítimas del tratamiento, aplicando en cada momento las técnicas más adecuadas para garantizar el equilibrio entre sus intereses y el mínimo impacto en los datos personales del afectado"[54].

Ahora bien, según el PLODP 2016, el principio de pertinencia implicaba que "los datos personales no podrían ser utilizados para fines distintos a los que motivaron su obtención" –art. 3.2–. Así también el PLODP 2019 caracterizó el principio de pertinencia y minimización de datos personales, señalando que "los datos personales deben ser pertinentes y limitados a lo mínimo necesario para su finalidad" –art. 12–[55]. Encontrándose, directamente, relacionado con el principio de calidad de datos, advertimos que "se puede hablar así de un *principio de adecuación*, que exige esta idoneidad de los datos recabados para la consecución de la finalidad. El termino pertinencia –"dícese de lo que viene a propósito"– abunda en esa idea de idoneidad y adecuación de los datos con la finalidad"[56].

[53] Por ejemplo, como señala la Guía Legislativa "los datos relativos a opiniones podrían ser fácilmente engañosos si se usan para fines con los cuales no guarden ninguna relación".
[54] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 349.
[55] Hay que considerar que la LOPD 15/1999 dentro del principio de calidad de datos, consideraba que los datos de carácter personal "no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos" –art. 4.2–.
[56] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 399.

Conforme el RGPD, el principio de pertinencia presenta una doble perspectiva. Por una parte, bajo el principio de limitación de la finalidad, se establece que los datos personales serán recogidos con unos fines determinados "y no serán tratados ulteriormente de manera incompatible con dichos fines" –art. 5.1. b)–. Y, por otra, bajo el principio de minimización de datos, se señala que los datos personales serán "adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" –art. 5.1. c)–. En cualquier caso, apuntamos que este principio encuentra una aplicación práctica "en la aplicación del principio de protección de datos desde el diseño, recomendando el propio Reglamento la implementación de medidas técnicas y organizativas destinadas a asegurar el menor impacto en la privacidad del interesado utilizando para ello, por ejemplo, la «seudonimización»"[57].

Llama la atención que la CCE caracterice el principio de pertinencia bajo el principio de utilidad, señalando que:

> Otro aspecto importante es el principio de utilidad, bajo el cual, la información constante en documentos, datos genéticos, bancos o archivos de datos, que reposa en entidades públicas o privadas, en soporte material o electrónico, debe cumplir una función específica, que implica la satisfacción de un interés legítimo determinado por la importancia y utilidad de la información (…) A ello va ligado, entonces, la responsabilidad de la entidad pública, llámese Instituto Ecuatoriano de Seguridad Social, IESS, de administrar la información en una base de datos confiable, que responda a principios de necesidad, veracidad, integridad, finalidad, utilidad, entre otros, puesto que la información que difunda debe ser veraz e imparcial, y sobre todo no puede vulnerar derechos fundamentales de los afiliados[58].

Entendemos que debido al carácter instrumental que tiene el derecho a la protección de datos, se observa la cardinal integración entre los principios de finalidad, utilidad, proporcionalidad, minimización de datos –y, en suma, de calidad de datos– con el de pertinencia. A nuestro parecer, el principio de pertinencia pudo concretarse en los proyectos de Ley general en Ecuador, a través del de calidad de datos[59]. Un principio, mucho más amplio, que permite que el tratamiento de la información

[57] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 349.

[58] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –CASO No.14-9-EP– publicada en el Registro Oficial Nro. 18 de 3 de septiembre de 2009.

[59] Hay que subrayar que, el PLODP 2019 reconoció como un principio para la protección de datos el principio de calidad, el cual señalaba que "los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros y, de ser el caso, debidamente actualizados, de tal forma que no se altere su veracidad" –art. 16–.

personal “sea adecuada, pertinente y no excesiva con relación a los fines del tratamiento”[60]. Por tanto, asegura una tutela, más integral sobre el derecho a la protección de datos. En todo caso, la LOPD regula por separado, tanto el principio de pertinencia y de minimización, por el cual “los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento” –art. 10. e)–; como el principio de calidad, el cual supone que “los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros” –art. 10. h)–. De este modo, atendiendo el modelo de regulación que plantea el RGPD, resaltamos que la LOPD recoge el principio de pertinencia dentro del principio de minimización de datos.

### 1.3 El principio de veracidad

Este principio, como parte del de calidad de datos, prevé ciertas condiciones como la exactitud o prohibición de exceso y, por tanto, exige “a los responsables comprobar la veracidad de los datos que recogen y la obligación de su puesta al día para que reflejen la realidad actual del afectado”[61]. En este caso, la CCE sostiene que:

> Las instituciones públicas, garantes de la Constitución de la República, están obligadas, en lo que respecta al manejo de información, a velar por la exactitud y fidelidad de los datos registrados, sea en medio manual o informático, por la legalidad en su recolección, por el seguimiento y su constante actualización, por la implementación de dispositivos que impidan accesos no autorizados, entre otros[62].

El principio de veracidad está vinculado con el principio de licitud, a partir de la recolección y posterior tratamiento de la información. Exige condiciones relacionadas con la exactitud, fidelidad y prohibición de exceso en el tratamiento de datos. Por lo cual, el tratamiento sería excesivo –afectando su veracidad, fidelidad y exactitud– cuando resulte que “determinados datos personales no son adecuados

[60] Enrique Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, (Madrid: Editorial Dykinson S.L, 2017), 227.
[61] Muñoz Ontier, “Disposiciones Generales (Arts. 1-5)”, 350.
[62] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –CASO Nro. 14-9-EP– publicada en el Registro Oficial Nro. 18 de 3 de septiembre de 2009.

–no sirven– para esa finalidad y que, por eso, son excesivos"[63]. De hecho, los EPEI, como parte del principio de calidad de datos, consideran que el responsable del tratamiento "adoptará las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento" –art. 19.1–. Asimismo, la Guía Legislativa de la OEA sugiere que, sobre la base del principio de calidad de datos, pertinencia y necesidad, "el recopilador o procesador de datos debe adoptar mecanismos para cerciorarse de que los datos personales sean correctos, exactos y completos y estén actualizados". En este marco, advertimos que, además, este principio comporta la adopción de mecanismos de actualización, de tal manera que los datos sean exactos, completos, actualizados y no excesivos, según la finalidad para la que fueron recabados[64]. Por tanto, "se exige, por tanto, al responsable que sea proactivo en la actualización de la información del afectado que consta en sus registros, pudiendo establecer incluso mecanismos técnicos para su actualización automática"[65].

Ahora bien, el PLODP 2016 señaló que, conforme el principio de veracidad, "la recolección de datos personales deberá ser veraz y no excesiva; no podrá obtenerse por medios fraudulentos, abusivos o en forma contraria a la presente Ley" –art. 3.3–; y, también el PLODP 2019 reconoció, dentro del principio de calidad, la garantía de la veracidad de los datos, señalando que éstos debían estar "debidamente actualizados; de tal forma que no se altere su veracidad" –art. 16–, lo

[63] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 400.
[64] Respecto a la calidad de datos, la Guía Legislativa de la OEA considera que, los datos "deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación. La exactitud, la pertinencia y la necesidad son principios cruciales de la protección de datos y la privacidad personal. Desde luego, sus requisitos deben evaluarse en relación con el contexto específico en el cual se recopilen, usen y divulguen los datos. Las consideraciones contextuales incluyen qué datos particulares se recopilan y con qué fines". De esta manera, en cuanto a la exactitud determina que los datos personales "deben ser correctos, exactos y completos y estar actualizados según sea necesario con respecto a los fines para los cuales se hayan recopilado. Evidentemente, la calidad de los datos es importante para la protección de la privacidad. Los datos inexactos pueden perjudicar tanto al procesador de datos como al titular de los datos, pero en una medida que varía mucho según el contexto".
[65] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 350.

cual implica que “el responsable deberá ser diligente en la rectificación de los datos del afectado cuando este así se lo requiera mediante el ejercicio de su derecho, pero, además, deberá hacer lo que esté en su mano para mantener actualizados sus registros”[66]. Así, lo ha ratificado el legislador en la LOPD al concretar que, mediante el principio de calidad y exactitud, los datos personales que sean objeto de tratamiento tienen que ser actualizados, de tal forma que no se altere su veracidad –art. 10. h)–.

Dentro de dicho tratamiento, advertimos algunas condiciones. Así, éste tiene que ser exacto, completo, actualizado y no excesivo de conformidad al contexto en el cual se recopilen, usen y divulguen los datos personales[67]. De este modo, recordando a la CCE, el responsable del tratamiento debe velar por la exactitud y fidelidad de los datos que se registren, atendiendo a los principios de licitud en su recolección y veracidad. Puede considerarse que todas estas condiciones integran el denominado principio de calidad de datos, por cuanto un fichero “tiene calidad cuando la tienen los datos y los datos tienen calidad cuando son exactos, cuando reflejan verazmente la realidad de la persona”[68].

Por otra parte, el RGPD considera que el tratamiento de datos debe responder al principio de exactitud y, por ello, “se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan” –art. 5.1 d)–. Al igual que la Guía Legislativa de la OEA, el RGPD relaciona el principio de veracidad con el de exactitud, garantizando que el tratamiento de la información no sea excesivo y que, por consiguiente, los datos sean exactos y actualizados, conforme a los fines para los cuales fueron recabados. En este sentido, “parece evidente que el primer interesado en mantener una ficha actualizada de los datos personales de sus

[66] Ibíd.

[67] Recordemos que la LOPD 15/1999 señalaba que los datos de carácter personal podían ser sometidos a tratamiento cuando no sean excesivos –art. 4.1–. En todo caso, esta Ley precisaba que el principio de calidad exige que los datos sean “exactos y puestos al día de forma que respondan como veracidad a la situación actual del afectado” –art. 4.3–.

[68] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 409.

usuarios sea el propio responsable para poder cumplir con las finalidades del modo más fiel posible"[69]. Por ello, esto obliga al responsable del tratamiento a contemplar "procedimientos de actualización de la información que la pongan permanentemente al día, garantizando la exactitud de la misma"[70].

En este orden, la LOPD completó el PLODP 2019, toda vez que la nueva normativa de protección de datos ha determinado que "se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan". Además, por una parte, si bien el PLODP 2016, determinó que los datos no podrían recogerse "por medios fraudulentos, abusivos o en forma contraria a la presente Ley"; consideramos que esta previsión formaba parte del contenido del principio de licitud. Y, por otra, es importante destacar que el PLODP 2019 enmarcó la necesidad de que los datos sean exactos, completos, actualizados y no excesivos a partir del principio de calidad de datos. En todo caso, según lo previsto en el art. 14 de la LOPD, es conveniente resaltar que a este principio le complementan las facultades de control e impugnación –derecho de rectificación– sobre el tratamiento de la información, cuando esta sea excesiva o inexacta, por cuanto el ejercicio de este derecho "exige que los datos de carácter personal sean exactos y puestos al día de forma que respondan con veracidad a la situación del afectado"[71].

### 1.4 El principio de confidencialidad e integridad: El deber de secreto y la seguridad de los datos

Tomando en consideración que el tratamiento debe responder a los fines legítimos, para los cuales fueron recabados; el carácter instrumental del derecho a la protección de datos precisa una tutela y garantía integral sobre el procesamiento, disposición, divulgación y confidencialidad de la información. Así, otro de los derechos y libertades que corresponde al titular de los datos personales es la

[69] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 350.
[70] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 409.
[71] Ibíd., 560.

confidencialidad, reserva o deber de secreto de la información. A partir, de estos principios resultan una serie de limitaciones y obligaciones para los responsables o encargados del tratamiento de la información, por cuanto se les exige "que traten los datos personales de tal manera que se garantice una seguridad adecuada de los mismos"[72]. Por una parte, los EPEI señalan que el principio de confidencialidad, exige que los responsables del tratamiento, no solamente adopten controles o mecanismos de protección sino también "mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular" –art. 23.1–. En primer término, señalamos que "este deber de secreto no es sólo individual, sino que es un deber colectivo que alcanza a todas las personas que conocen la información"[73]. Por ello, el respeto de este principio implica que el manejo de la información personal se debe ajustar a una serie de mecanismos de protección basados en un entorno seguro y controlado, tendente a garantizar que los datos no puedan revelarse.

En este orden de cosas, la CCE precisa que:

> En la actualidad, nuestra vida está registrada en instituciones públicas y privadas y, en la mayoría de los casos, no conocemos exactamente el contenido de esa información sobre nosotros mismos o sobre nuestros bienes. Muchas veces es información incorrecta por falta de actualización de tales registros o bancos de datos, y al circular esa información incorrecta, perjudica la honra y buena fama, es decir, se trata de una información relacionada a hechos privados e íntimos que, al ser divulgada, vulneraría el ámbito de la privacidad, precisamente, por el carácter de confidencialidad de tal información[74].

Frente a la divulgación no autorizada, los derechos de control y dominio de la información que asigna el *habeas data,* permiten asegurar a los ciudadanos facultades, –entre ellas el deber de secreto o confidencialidad–, conducentes a exigir de los responsables del tratamiento una protección adecuada. Así, observamos que "esta obligación está, a su vez, vinculada con el propio interés legítimo del responsable en el sentido de que el esfuerzo que realice para garantizar la seguridad de la información ha de ser proporcionado"[75]. En todo caso, "si bien

[72] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 350.
[73] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 497.
[74] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –CASO Nro.14-9-EP– publicada en el Registro Oficial Nro. 18 de 3 de septiembre de 2009.
[75] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 350.

quien debe tratar datos personales está obligado a la transparencia respecto a los que pretende recoger y a las finalidades del tratamiento, en cuanto lo inicia también contrae el compromiso de garantizar la confidencialidad"[76].

Sobre este respecto, también anotamos que la CCE reconoce como una dimensión utilitaria del *habeas data* el derecho de reserva o confidencialidad, señalando que ésta persigue "asegurar que la información recabada sea entregada única y exclusivamente a quien tenga autorización para ello"[77]. Nos encontramos frente a un principio esencial del marco de regulación para la protección de datos y que, igualmente, compromete la actividad que desempeñan los responsables, como una obligación complementaria del deber de secreto profesional. Por ello, como precisa la CCE, es necesario que la Administración Pública desempeñe sus actividades con eficiencia y responsabilidad, frente a la protección y garantía de los derechos y libertades fundamentales. Así pues, no debe olvidarse que "entre los fines esenciales del Estado están los de servir la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución[78]. Si bien la Constitución, prescribe que "no existirá reserva de información" –art. 18.2–, la cual se encuentre en poder de la Administración Pública, al mismo tiempo señala que, excepcionalmente, este principio sí aplica "en los casos expresamente establecidos en la Ley".

Como se ha señalado, el derecho a la protección de datos y *habeas data* configuran un instituto de garantía destinado a precautelar, no solamente la tutela de la intimidad de la información personal sino también a ejercer algunas facultades de control y dominio sobre el tratamiento. De manera que, este derecho representa una limitación, frente a la divulgación de esa información conforme a la dimensión utilitaria de secreto y/o confidencialidad.

[76] Ramon Oró, *La protección de datos*, 66.

[77] Véase la Resolución de la Corte Constitucional 182, Sentencia Nro. 182-15-SEP-CC –CASO Nro. 1493-10-EP– publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015.

[78] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –CASO Nro. 14-9-EP– publicada en el Registro Oficial Nro. 18 de 3 de septiembre de 2009.

Por otra parte, el PLODP 2016 especificó que "tanto el responsable como el usuario de bases de datos debe adoptar medidas para resguardar de manera confidencial los datos personales, con el objeto de evitar su adulteración, pérdida o tratamiento no autorizado" –art. 3.5–. Así también, sobre la base del art. 15 del PLODP 2019, la LOPD ha reconocido que el principio de confidencialidad en el tratamiento de datos, se concreta en el sigilo y secreto de la información "es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme a los supuestos de tratamiento legítimo señalados en esta Ley" –art. 10. g)–.

Ahora bien, aunque este principio está destinado a garantizar el carácter confidencial de los datos personales durante el tratamiento, además, el deber de secreto o sigilo de la información subsiste, aún después, de finalizar las relaciones entre los responsables y el titular de los datos. En consecuencia, "dichas obligaciones se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento"[79]. Es conocido que el uso ilícito de la información –incluso, actos discriminatorios–, pueden suceder, aún después, del tiempo en que los datos fueron requeridos para su tratamiento. Por ello, como señala la Guía Legislativa de la OEA, un elemento esencial para el respeto del principio de confidencialidad de la información es "el establecimiento y mantenimiento de la confianza entre el titular de los datos y el controlador de datos, especialmente con respecto a la divulgación de datos personales a terceros*".*

Sobre este principio, el RGPD considera que dentro del tratamiento de datos se debe garantizar "una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas" –art. 5.1 f)–. Evidenciamos que, como una obligación de los encargados del tratamiento, el RGPD establece que se debe garantizar "que las personas autorizadas para tratar datos personales se hayan comprometido a

[79] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 350.

respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria" –art. 28.3 b)–. Finalmente, apreciamos que –al tenor del RGPD– la LOPDGDD reconoce que todas las personas que intervienen en cualquier fase del tratamiento "estarán sujetas al deber de confidencialidad (…) será complementaria de los deberes de secreto profesional (…) se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento" –art. 5–[80].

Al mismo tiempo, el art. 5 de la PLOPD 2016 destacaba que, conjuntamente, al deber de secreto, debía garantizarse la seguridad de la información, a través de medidas que impidieran la adulteración o pérdida de la información. En este caso, advertimos que, además, el PLOPD 2019 reconoció dentro del principio de confidencialidad, por una parte, el mantenimiento de la seguridad de los datos –art. 15 *in fine*–; y, por otra, como un principio independiente a la seguridad de datos personales, por el cual, el responsable y encargado tendrían que "implementar todas las medidas de seguridad adecuadas y necesarias, sean técnicas, organizativas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, acceso no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita" –art. 18–. Dos supuestos que, finalmente, el legislador ha ratificado en la LOPD al determinar que "el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio" –art. 10. g) *in fine*–; e, "implementar todas las medidas de seguridad adecuadas y necesarias (…) para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto" –art. 10. j)–.

En este marco, como precisa el RGPD, vinculado a la confidencialidad, pero, independiente a la vez, se encuentra el deber de garantizar la integridad de la información, por medio, de seguridades adecuadas. Así, por ejemplo, se destacan

[80] La LOPD 15/1999 señalaba a este principio como un deber de secreto, por el cual, los responsables del tratamiento de datos, y demás que intervengan en sus distintas fases, "están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo" –art. 10–.

“la seudonimización y el cifrado de datos personales” –art. 32.1. a)–; “la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento” –art. 32.1. b)–; “la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico” –art. 32.1. c)–; y “un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento” –art. 32.1. d)–.

> De esta forma, «el Reglamento se aleja de un modelo jurídico de Derecho continental europeo, que proviene del Derecho romano y que se caracteriza por una amplia regulación y una predeterminación de la solución jurídica, para acercarse más a un modelo de Common Law, que se caracteriza por una mayor desregulación y que tiene en cuenta la valoración del caso concreto. Esto se pone de manifiesto especialmente en las medidas de seguridad de los tratamientos (…) Evidentemente, la introducción de elementos de la cultura jurídica anglosajona, como la autorregulación, la desregulación y la accountability, si bien aporta una mayor flexibilidad a la hora de buscar soluciones al caso concreto y de adaptarse a los futuros cambios tecnológicos, también supone, como acabamos de señalar, una mayor inseguridad jurídica para aquellos responsables acostumbrados a la detallada y extensa regulación característica del modelo jurídico continental»[81].

Con referencia a este punto, la LOPD –siguiendo la línea del RGPD–, en primer término, determina que tanto el responsable como el encargado del tratamiento deberán implementar “un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos” –art. 37–. Y, además, identifica las medidas, que aquellos deben demostrar, frente a los riesgos en el tratamiento de datos. A saber: “anonimización, seudonimización o cifrado de datos personales” –art. 37.1–; “la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales” –art. 37.2–; “la resiliencia técnica, física, administrativa, organizativa y jurídica” –art. 37.3–. En todo caso, la LOPD difiere del RGPD, por cuanto este primer orden jurídico señala como una medida de seguridad la implementación, tanto de la “anonimización” como de la “seudonimización”, mientras que el segundo, únicamente, la “seudonimización”. Tomando en cuenta que la anonimización

[81] Antonio Troncoso, “Del principio de seguridad de los al derecho a la seguridad digital”, *Revista Economía Industrial*, Nro. 410 (2018):127-151.

constituye un procedimiento de disociación absoluta o definitiva, el cual impediría la identificación del titular de los datos y, por tanto, supondría la imposibilidad de que exista un tratamiento[82]; lo correcto sería que la LOPD considere tan solo a la seudonimización como una medida de seguridad, por cuanto –al tenor del RGPD– los datos seudonimizados pueden ser atribuidos a una persona, por medio del uso de información adicional.

Ahora bien, el PLODP 2016 requería una reformulación sobre el principio de confidencialidad e integridad, toda vez, que las referencias que se hacían no correspondían a la naturaleza del principio de confidencialidad, sino de exactitud e integridad. En el texto que se proponía se advertía que los responsables y encargados debían adoptar medidas de seguridad, que permitan resguardar lícita e, íntegramente, los datos personales objeto de tratamiento[83]. Además, a pesar de que el PLODP 2016 enunciaba como dos principios distintos a la confidencialidad y reserva, según la normativa europea se trata de un solo presupuesto destinado, por un lado, a establecer confianza en todo el proceso que implica el tratamiento de la información personal, y por otro, a resguardar y respetar el carácter reservado de los datos. Del texto que proponía el PLODP 2016, acerca del principio de reserva, se desprende que "las personas naturales o jurídicas que obtengan legítimamente información proveniente de una base de datos están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de sus actividades, siendo prohibida la difusión a terceros" –art. 3.6–. Así pues, si bien se hizo referencia

[82] Para que opere el derecho a la protección de datos debe existir un tratamiento y que, en efecto, este se sustancie sobre información personal.

[83] Para el cumplimiento de este deber, la Guía Legislativa de la OEA precisa que el controlador de datos debe asegurarse que, "no se proporcionen tales datos (ni se pongan a disposición por otros medios) a personas o entidades excepto con el conocimiento o consentimiento de la persona afectada, en consonancia con las expectativas razonables de la persona afectada o por mandato de la Ley (…) Estas responsabilidades emanan de la naturaleza misma de los datos personales y no dependen de afirmaciones de las personas afectadas. Este deber de respetarlos límites de la divulgación se suma a la obligación de los controladores de datos enunciada en el principio seis de promover la seguridad externa e interna y el cumplimiento de la normativa al salvaguardar los datos. Proteger la privacidad implica no solo mantener la seguridad de los datos personales, sino también permitir que las personas controlen la forma en que se usan y divulgan sus datos personales".

a utilizar la información de forma reservada, la naturaleza que describe el texto legal corresponde al principio de finalidad[84].

Recordando que la CCE insiste en que el derecho a la protección de datos "implica la necesidad de garantizar la protección de la esfera íntima de las personas, así como la posibilidad de ejercer control sobre los datos personales del sujeto, aunque no se encuentren en su poder"[85]; y así también que una de las dimensiones utilitarias para ejercer ese control es el derecho de reserva o confidencialidad que tiene por objeto "asegurar que la información recabada sea entregada única y exclusivamente a quien tenga autorización para ello"[86]. Advertimos que, el PLODP 2016 confundió el principio de reserva con el principio de confidencialidad. En todo caso, conforme a la LOPD, subrayamos que, tanto la confidencialidad como la seguridad de los datos personales se encuentran ordenados bajo un mismo principio, el cual enmarca el deber de secreto de los responsables y encargados, antes y después del tratamiento de la información.

### 1.5 El principio de transparencia e información al interesado

Como hemos destacado, el RGPD reconoce que los datos personales serán tratados "de manera lícita, leal y transparente en relación con el interesado" –art. 5.1. a)– [87]. Entendemos que de un tratamiento lícito, leal y transparente se

[84] En otros contextos jurídicos, el principio de finalidad es entendido como aquel que "define qué datos se pueden recoger y cuáles no porque unos datos pueden ser adecuados para una finalidad, pero no para otra. Este principio de finalidad exige tres elementos: la legitimidad, la determinación y la explicitud". Cfr. Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 396.

[85] Véase la Resolución de la Corte Constitucional 1, Sentencia Nro. 1-14-PJO-CC –CASO Nro. 67-11-JD– publicada en el Registro Oficial Suplemento Nro. 281 de 3 de julio de 2014.

[86] Véase la Resolución de la Corte Constitucional 182, Sentencia Nro. 182-15-SEP-CC –CASO Nro. 1493-10-EP– publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015.

[87] El RGPD advierte que "los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación

desprende la obligación de poner en conocimiento del interesado cuanta información sea necesaria sobre la existencia de un tratamiento y los fines para los cuales los datos personales serán tratados[88]. De esta manera, el principio de transparencia "condiciona lógicamente la capacidad del individuo para hacer efectiva la garantía de protección que establece el ordenamiento. Evidentemente, si el interesado no dispone de la información relativa al tratamiento de sus datos, difícilmente podrá materializarse la esencia de este derecho"[89].

El PLODP 2016 incluyó dentro del principio denominado como "consentimiento informado", la garantía de que el interesado o titular de los datos personales prestara el consentimiento para tratar sus datos personales, de manera "libre, expresa, previa e informada" –art. 3.4–. No obstante, de un modo más preciso, recordemos que el PLODP 2019 reconoció que "las relaciones derivadas del tratamiento de datos personales deben ser transparentes" –art. 9–. En todo caso, encontramos que la LOPD desarrolla este principio ampliamente al determinar que el tratamiento de datos "deberá ser transparente, por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro"; y por tanto, las relaciones derivadas del tratamiento "deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia" –art. 10. c)–.

---

con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente" –Considerando 60–.

[88] Además, el RGPD agrega que "se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general" –Considerando 61–.

[89] Javier Aparicio Salom, "Derechos del interesado (Arts. 12-19)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 363.

Ahora bien, en el marco internacional la LOPDGDD reconoce que "cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información" –art. 11.1–[90]. Así pues, por una parte, la transparencia como derecho "a la información en la recogida de los datos –manifestación del derecho fundamental a la protección de datos– es distinto a otros derechos a la información que tiene el ciudadano, mucho más amplios y que están vinculados a otros bienes jurídicos"[91]; y por otra, como un principio del tratamiento de datos, "la transparencia debe caracterizar íntegramente en el tratamiento de datos y el responsable del tratamiento debe llevar a cabo el tratamiento de los datos conforme a este principio y, además deberá acreditar que trata los datos transparentemente"[92]. Así, como destaca la Guía Legislativa de la OEA, este principio supone "informar a las personas sobre las prácticas y políticas de las entidades o personas que recopilen los datos personales, a fin de que puedan tomar una decisión fundamentada con respecto al suministro de tales datos".

En este orden, los EPEI establecen que "el responsable informará al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto" –art. 16.1–. Por tanto, advertimos que este principio exige que el titular de los datos "conozca toda la información que resulte precisa para garantizar la lealtad del tratamiento. En este sentido, debe facilitarse información sobre los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del procedimiento para hacer valer sus derechos en relación con el mismo"[93].

[90] El Preámbulo de la LOPDGDD aclara que "el Título III, dedicado a los derechos de las personas, adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información".
[91] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 453.
[92] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 364.
[93] Ibíd., 365.

Desde esta perspectiva, si bien los proyectos de Ecuador hacían referencia al consentimiento informado y a la transparencia como garantías para la licitud y lealtad del tratamiento de la información, al parecer dichas prescripciones, resultaban insuficientes a la hora de regular la obligación que tienen los responsables del tratamiento, en cuanto al deber de informar al titular de los datos sobre la existencia de un tratamiento. En todo caso, si bien el art. 12 *in fine* de la LOPD determina que, con el objeto de garantizar el derecho a la información, ésta debe ser proporcionada al titular de los datos "de forma accesible por cualquier modo comprobable en un lenguaje claro, sencillo y de fácil comprensión, de preferencia propendiendo a que pueda ser accesible en la lengua de su elección"; el legislador, ha omitido el detalle de cómo se cumplirá cada uno de los presupuestos o momentos, que comprende el principio de transparencia[94].

### 1.6 El principio de responsabilidad proactiva

Los principios del derecho a la protección de datos tienen por objeto ordenar la aplicación de la normativa a un conjunto de reglas que garanticen claridad, coherencia, confianza y seguridad jurídica. En este orden, el principio de responsabilidad proactiva "implica que el responsable del tratamiento tiene que garantizar la licitud, la lealtad y la transparencia en todo el proceso del tratamiento

[94] Así, atendiendo al momento en que se hace efectivo el principio de transparencia, "cabe diferenciar dos momentos. En primer lugar, en el momento en que el responsable asume la capacidad de decisión sobre los datos de la persona, momento en el que nace la obligación de informar acerca de las características del tratamiento que tiene intención de llevar a efecto. Este supuesto es el que se denomina deber de información. En segundo lugar, está el supuesto de transparencia sobrevenida, que obliga al responsable a informar al interesado acerca de las nuevas circunstancias tan pronto como sucede algún cambio esencial en el tratamiento, a facilitar a los interesados la información sobre el tratamiento cuando éstos piden tener acceso a la misma, o, por último, a facilitar información relativa a la tramitación y decisión de las solicitudes de rectificación, supresión y oposición y demás derechos derivados del principio de transparencia. El supuesto de información sobrevenida sucede en el momento en que el que una entidad, que ya explota los datos de carácter personal mediante un tratamiento constituido legítimamente, tiene intención de servirse de la información para un propósito adicional, diferente de aquellos que perseguía hasta ese momento o bajo unas condiciones o circunstancias diferentes de las que ya conoce el interesado y que resultan adecuadas a las garantías normativas". Cfr. Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 365.

de datos con relación al interesado"[95] y, por tanto, "están obligados a establecer, proceso por proceso de tratamiento, aquellas medidas que consideren mínimamente apropiadas para garantizar la confidencialidad y protección de la información"[96]. En tal sentido, el RGPD dispone que "el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo" –art. 5.2–. Así también los EPEI apuntan que, bajo el principio de responsabilidad el responsable del tratamiento, "implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones (…) rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control" –art. 20.1–[97].

Aunque el PLODP 2016, no reconoció el principio de responsabilidad proactiva, conforme el modelo que plantea el Estado constitucional de derechos y justicia, la protección de datos personales supone que los responsables del tratamiento deben respetar (principio de eficacia directa) las garantías y principios constitucionales previstos para el derecho a la protección de datos[98]. En este sentido, subrayamos que este principio exige del responsable "poder acreditar en todo momento que ha llevado a cabo correctamente sus obligaciones y que mantiene al día la adecuación efectuando los procedimientos de actualización y control de cumplimiento necesarios"[99]. Ahora bien, basándose en el art. 19 del PLODP 2019, la LOPD ha reconocido a la responsabilidad proactiva y demostrada como un principio, en el

[95] Puyol Montero, "Los principios del Derecho a la Protección de Datos", 140.

[96] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 351.

[97] Los EPEI reconocen la importancia de la adopción de medidas preventivas que "permitan al responsable responder proactivamente ante los posibles problemas relacionados con el derecho a la protección de datos personales como son la adopción de esquemas de autorregulación vinculante o sistemas de certificación en la materia; la designación de un oficial de protección de datos personales; la elaboración de evaluaciones de impacto a la protección de datos personales y la privacidad por defecto y por diseño, entre otras, lo cual resulta esencial en el ámbito de las tecnologías de la información y las telecomunicaciones" –Considerando 23–.

[98] Recordemos que la Guía Legislativa de la OEA advierte la necesidad de que "en las Leyes nacionales sobre privacidad se debe exigir que los controladores de datos rindan cuenta del cumplimiento de estos principios. Además del mecanismo con que cuenten las autoridades gubernamentales para hacer cumplir la normativa, el derecho interno debe proveer a las personas de mecanismos apropiados para responsabilizar a los controladores de datos de las violaciones que se produzcan (por ejemplo, mediante la indemnización por daños y perjuicios)".

[99] Muñoz Ontier, "Disposiciones Generales (Arts. 1-5)", 351.

que el responsable del tratamiento de datos personales “deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley” –art. 10. k)–[100]. Desde esta perspectiva, es importante anotar que –al igual que el RGPD–; esta propuesta obliga o impone al responsable acreditar que el tratamiento garantiza la licitud, la lealtad y la transparencia en el derecho a la protección de datos.

### 1.7 Tratamiento de categorías especiales de datos personales

El tratamiento de categorías especiales o datos personales sensibles merecen un análisis distinto a las categorías generales de datos personales. Hay que reiterar que “la definición de estos datos como especialmente protegidos tiene consecuencias, sobre todo en lo que hace referencia al consentimiento para el tratamiento, así como en la determinación de las medidas de seguridad aplicables, que deben ser de nivel alto”[101]. Por ello, siguiendo el ejemplo que plantea el RGPD, “la ubicación sistemática en preceptos distintos de la regulación del tratamiento de las categorías especiales de datos personales y de las categorías generales de datos personales responde a su distinto régimen jurídico”[102].

En el tratamiento de esta tipología de datos, –en cuanto al consentimiento–, destacamos, nuevamente, la importancia del derecho de información que asiste al titular de los datos; y, además, en relación a las medidas de seguridad de los datos, la necesidad de prever las distintas obligaciones que pesan sobre el responsable del tratamiento. Sobre este aspecto, la CCE describe que una de las dimensiones utilitarias del *habeas data,* –orientada a garantizar la seguridad de la información–,

[100] El PLODP agrega que, dicha acreditación se podrá realizar valiéndose de “estándares, mejores prácticas, esquemas de auto y corregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento” –art. 19–.
[101] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 467-468.
[102] Troncoso, “Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales”, 226.

es la dimensión denominada como "*habeas data cancelatorio*" o derecho a la exclusión de información sensible, que "busca que la información considerada sensible sea eliminada, por no ser susceptible de compilación"[103].

Con referencia a este aspecto, el RGPD manifiesta una prohibición de tratar datos personales que revelen "el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física" –art. 9.1–[104].

Conviene señalar que el PLODP 2016 estimó una prohibición sobre el tratamiento de datos sensibles, "en todo aquello que pueda afectar el derecho a la intimidad de la persona" –art. 5–. Esta norma expuso que, nadie podía ser obligado a proporcionar datos sensibles, salvo cuando: el titular de los datos, autoriza el tratamiento de manera expresa y por escrito (explícito según el RGPD) –art. 5.1–; es necesario para salvaguardar un interés vital o legítimo; 3) se refiere a datos indispensables en procesos judiciales; y 4) tiene una finalidad estadística, científica o académica –art. 5.2–. En este ámbito, el PLODP 2019 refirió el consentimiento como la única habilitación para el tratamiento de datos sensibles. Es decir, "la

[103] Véase la Resolución de la Corte Constitucional 182, Sentencia Nro. 182-15-SEP-CC –CASO Nro. 1493-10-EP– publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015.

[104] Al respecto, el RGPD menciona que: "especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física (…) Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales" –Considerando 51–.

manifestación de la voluntad explícita del titular" –art. 39–, garantizando que, a través del principio de proporcionalidad el tratamiento sea "adecuado, necesario, oportuno, relevante y no excesivo en relación a las finalidades para las cuales han sido recogidas o a la naturaleza de las categorías especiales" –art. 13–.

Sin embargo, siguiendo los preceptos del art. 9 del RGPD, la LOPD ha establecido un conjunto de excepciones, las cuales habilitan el tratamiento de datos sensibles, cuando: "el titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines" –art. 26. a)–; "el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social" –art. 26. b)–; "el tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento" –art. 26. c)–; "el tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos" –art. 26. d)–; "el tratamiento se lo realiza por orden de autoridad judicial" –art. 26. e)–; "el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular" –art. 26. f)–; y "cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente ley" –art. 26. g)–.

De este modo, el tratamiento de datos sensibles debe atender, principalmente, a criterios de legitimación dentro de su tratamiento, ya que, por regla general y mandato constitucional, salvo las excepciones planteadas, nadie puede ser obligado a declarar sobre esta tipología de datos[105]. La Constitución de Ecuador reconoce como un derecho de libertad de todas las personas "el derecho a guardar

[105] Como apunta la Guía Legislativa de la OEA, el consentimiento explícito "a la cual se refieran los datos debe ser la regla que rija la recopilación, la divulgación y el uso de datos personales sensibles. Al determinar las obligaciones reglamentarias pertinentes, hay que tener en cuenta el contexto en el cual una persona proporciona esos datos".

reserva sobre sus convicciones" –art. 66.11–. Según esta disposición, "nadie podrá ser obligado a declarar sobre las mismas"; de modo tal que, "en ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica"[106]. Precisamente, en la línea general de los datos sensibles existe una limitación o restricción en su tratamiento, requiriéndose un mayor nivel de protección[107]. En todo caso, si bien el PLODP 2016 planteó que exista una prohibición de tratar datos personales sensibles "en todo aquello que pueda afectar la intimidad de la persona" –art. 5–, existía un error que debía subsanarse. El derecho a la protección de datos se consagra como un instituto de garantía de otros derechos, que afecta al desarrollo de la personalidad. Por tanto, no solamente se hace referencia a la protección de la intimidad de la persona[108].

Ahora bien, dentro de la categoría de datos sensibles puede, excepcionalmente, existir la posibilidad de recabar información personal, a partir del consentimiento que preste el titular de los datos o su legítimo representante. En este orden, el art. 9.2 del RGPD presenta una lista extensa de los casos en los que no aplica la prohibición del tratamiento de datos sensibles. Por ejemplo, en relación al interesado, cuando éste "dio su consentimiento explícito para el tratamiento de

[106] Como hemos señalado anteriormente, debe tenerse en cuenta que, en la Constitución de Ecuador uno de los principios para el ejercicio de los derechos es que "todas las personas son iguales y gozaran de los mismos derechos, deberes y oportunidades" –art. 11.2–. Por tanto, "nadie podrá ser discriminado por razones de etnia, lugar de nacimiento, edad, sexo, identidad de género, identidad cultural, estado civil, idioma, religión, ideología, filiación política, pasado judicial, condición socio-económica, condición migratoria, orientación sexual, estado de salud, portar VIH, discapacidad, diferencia física; ni por cualquier otra distinción, personal o colectiva, temporal o permanente, que tenga por objeto o resultado menoscabar o anular el reconocimiento, goce o ejercicio de los derechos".

[107] En este punto, la Guía Legislativa de la OEA determina que: "los controladores de datos deberían adoptar medidas de privacidad y de seguridad que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los individuos sujetos de la información (…) Debe recaer en los controladores de datos la carga de determinar los riesgos importantes para los titulares de los datos como parte del proceso general de gestión de riesgos y evaluación del impacto en la privacidad. Si se responsabiliza a los controladores de datos, se podrá proteger mejor a los titulares de los datos contra daños considerables en una amplia gama de contextos culturales".

[108] A partir del texto que se propone en Ecuador y, en virtud, del instituto de garantía que se desprende del derecho a la protección de datos, la intimidad no significa el único concepto conexo a la protección de bienes jurídicos, que pueden afectarse en el tratamiento de la información.

dichos datos personales con uno o más de los fines especificados" –art. 9.2. a)–; y también cuando "se refiere a datos personales que el interesado ha hecho manifiestamente públicos" –art. 9.2. e)–. Asimismo, la prohibición que señala el RGPD no será de aplicación en los casos de: "cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social" –art. 9.2. b)–; "proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento" –art. 9.2. c)–; "la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial" –art. 9.2. f)–; "fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social" –art. 9.2. h)–; "razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios" –art. 9.2. i)–; y, "fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos" –art. 9.2. j)–.

En relación a la regulación del tratamiento de los datos sensibles, desde el RGPD se evidencia un panorama más amplio, en virtud de materializar una tutela más adecuada de los derechos que corresponden al interesado o titular. En este sentido, enfatizamos que "la limitación a unos supuestos concretos del tratamiento legítimo de categorías especiales de datos personales es coherente con el principio general de prohibición del tratamiento de estas categorías de datos"[109]. Esto es importante, por cuanto los datos sensibles:

> Son datos que pertenecen a la esfera personal o intima de una persona –es una información que se reserva para uno mismo o para los más cercanos- y su conocimiento afecta

[109] Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", 227.

> gravemente a la intimidad personal y familiar y al libre desarrollo de la personalidad, teniendo un enorme potencial discriminador[110].

Finalmente, hay que destacar que el art. 9 de la LOPDGDD, a los efectos de la normativa expuesta en el RGPD, dispone que:

> 1. A fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.
>
> 2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del RGPD deberán estar amparados en una norma con rango de Ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.
>
> En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

En definitiva, los datos sensibles merecen especial protección, por cuanto en el contexto de su tratamiento pueden resultar graves afectaciones a los derechos y libertades de las personas. Por ejemplo, discriminación en razón de sus creencias políticas, religiosas u origen racial o étnico. Su tratamiento implica importantes consecuencias vinculadas al consentimiento, al interés público y protección de intereses vitales del titular de los datos. Tomando en consideración las disposiciones de la LOPDGDD, es esencial adecuar la aplicación de estos supuestos en la normativa sectorial, con el objeto de garantizar la seguridad jurídica y establecer requisitos relacionados, con las medidas de seguridad y confidencialidad.

## 2. Derechos de los Titulares

El ejercicio de los derechos de acceso, de rectificación, a la cancelación, oposición, limitación del tratamiento, portabilidad e información sobre las decisiones automatizadas, se constituyen como facultades de control y favorecen a los principios de transparencia y calidad de la información personal. “Todos estos derechos se relacionan entre sí en su relevancia, pues constituyen las herramientas

[110] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 782.

esenciales para hacer efectivos la mayoría de los principios y, además, por el hecho de que deben atenderse de forma transparente, informando al interesado"[111].

La garantía de estos derechos, no solo involucra el respeto de la intimidad de la información o de los bienes jurídicos que se desprenden del tratamiento, sino que, además, reconoce algunas dimensiones utilitarias incardinadas con el ejercicio de los derechos ARCO. Así, lo advierte la CCE cuando señala que, a partir del derecho a la protección de datos y del *habeas data*, "la persona titular de los datos podrá solicitar al responsable el acceso sin costo a la información a fin de conocer su contenido, lo cual, a su vez, le permitirá solicitar su actualización, rectificación, eliminación o anulación"[112]. En este orden, en primer término, advertimos que:

> El derecho de acceso consiste en obtener, sin restricciones, con una periodicidad razonable y sin atrasos ni gastos, la comunicación en forma inteligible de aquellos datos sobre uno mismo que sean objeto de un tratamiento (…) el derecho de rectificación obliga a que se modifiquen los datos personales inexactos o incompletos para conseguir que reflejen de forma fiel la realidad, el derecho de cancelación da lugar a que se suprima el tratamiento de aquellos datos que resulten ser inadecuados o excesivos; o bien de todos aquellos de los que se disponga, en caso de incumplir las normas que legitiman el tratamiento[113].

Por ello, la CCE insiste en que:

> Se accede a la información, se verifica la exactitud de la información del que la posee, se verifica qué uso está dando el poseedor a dicha información, se le impide que la difunda si ésta es errada, se cambia la información si es equivocada y se difundiría la verdadera información entre aquellos a quienes se emitió inicialmente, con el propósito de garantizar eficazmente los derechos constitucionales vinculados al honor, a la intimidad y a la buena fama[114].

Dentro de un Estado constitucional de derechos y justicia, la máxima realización de los derechos se concreta, a través de los poderes públicos, mediante sus diversos mecanismos de actuación[115]. Por ello, en esta parte final consideramos necesario

---

[111] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 363.

[112] Véase la Resolución de la Corte Constitucional 182, Sentencia Nro. 182-15-SEP-CC –CASO Nro. 1493-10-EP– publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015.

[113] Ramon Oró, *La protección de datos*, 68.

[114] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –CASO Nro.14-9-EP– publicada en el Registro Oficial Nro. 18 de 3 de septiembre de 2009.

[115] En el marco de protección y garantía efectiva del derecho a la protección de datos, los EPEI se promueven para "adoptar un marco regulatorio que reconozca a cualquier persona física, en su carácter de titular de sus datos personales, la posibilidad de ejercer, por regla general de manera gratuita y excepcionalmente con costos asociados por razones naturales de reproducción, envío, certificación u otras, los derechos de acceso, rectificación, cancelación, oposición y portabilidad,

realizar algunas reflexiones sobre el alcance y la naturaleza de los derechos o facultades de control y dominio que, incardinados al principio de transparencia, resaltan "la correspondiente obligación del responsable del tratamiento de facilitar al interesado la información completa sobre el tratamiento"[116].

Los EPEI reconocen que, como parte del principio de transparencia en el tratamiento de datos, deben coexistir mecanismos o procedimientos, que permitan el ejercicio de los derechos de acceso, rectificación, cancelación, portabilidad, oposición y decisiones automatizadas –art 16.2. d)–. Si tomamos en cuenta que el derecho a la protección de datos trata de impedir que el uso incorrecto de la información lesione algún derecho fundamental; el principio de transparencia se introduce en estos derechos como una fórmula para garantizar que el tratamiento de la información tenga "una finalidad concreta capaz de justificar la recopilación de los datos suficientes y proporcionados"[117]. Por tanto, todo tratamiento indeterminado o ilícito permite accionar mecanismos de impugnación, que forman parte del contenido esencial del derecho a la protección de datos.

En el contexto ecuatoriano, los arts. 12.14, 12.15 y 12.17 de la LOPD –arts. 6.1 del PLODP 2016 y art. 23.14 del PLODP 2019– reconocen a los titulares de los datos las facultades de control de éstos, por medio del ejercicio, no solamente de los derechos ARCO sino, además, de las limitaciones al tratamiento; a no ser objeto de una decisión basada, únicamente, en valoraciones automatizadas, incluida la elaboración de perfiles; y derecho a la portabilidad. Este reconocimiento es esencial, ya que, como apuntamos:

> Hay que destacar de forma especial los derechos de acceso, rectificación, cancelación y oposición que forman parte, como ha determinado la jurisprudencia constitucional, del contenido esencial del derecho fundamental a la protección de datos personales a la luz de la opinión generalmente admitida de los que este derecho significa –sin los cuales este derecho no es reconocible como perteneciente a su tipo previo– y sin cuyo ejercicio los intereses jurídicos que dan vida a este derecho resultan desprotegidos[118].

---

inclusive en el contexto de tratamientos de datos personales efectuados por motores o buscadores de Internet; derechos que complementan las condiciones necesarias para que los titulares ejerzan de manera plena su derecho a la autodeterminación informativa" –Considerando 19–.

[116] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 366.

[117] Ramon Oró, *La protección de datos*, 65.

[118] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 548**.**

Siendo necesario, además, el reconocimiento de los derechos de limitación del tratamiento, portabilidad e información sobre las decisiones automatizadas, la legislación de protección de datos debe garantizar el derecho a impugnar aquellos tratamientos que no cumplan con las finalidades y principios previstos para el tratamiento de datos.

> Por ello, sin perjuicio de que la doctrina que limita la transparencia a la necesidad de informar para la validez del consentimiento siga siendo perfectamente aplicable, debe abandonarse la idea de que la transparencia afecte y condicione preferentemente el consentimiento. Es preciso contemplar la transparencia como un elemento que afecta a la totalidad del tratamiento de datos, que en ningún caso podrá llevarse a efecto de forma poco transparente, puesto que esto afectará negativamente a su lealtad[119].

Así, el PLODP 2016 reconoció como un derecho de los titulares "conocer, actualizar, rectificar sus datos personales frente a los responsables o encargados del tratamiento" –art. 6.1–; y el PLODP 2019 reconoció el derecho a ser informado sobre "la existencia y forma en la que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas" –art. 23.14–. Esta prescripción ha sido adoptada por el legislador a la luz del art. 12.14 de la LOPD. Como hemos advertido en otro momento, aunque el PLODP 2016 se limitaba, únicamente, a enunciar el reconocimiento de los derechos ARCO, sin precisar una definición de cada una de estas facultades; el PLODP 2019, a partir del reconocimiento de las facultades de control de la información señaladas en el art. 23.14, en otras disposiciones, recogió la esencia de cada una de ellas[120].

Ahora bien, el PLODP 2016 propuso que el titular ejerciera el derecho a "ser informado por el responsable o el encargado del tratamiento, previa solicitud, respecto del uso que les ha dado a sus datos personales*"* –art. 6.2–*.* Asimismo, sobre la base del art. 23 del PLODP 2019, la LOPD ha establecido que el titular tiene derecho a conocer y a obtener del responsable del tratamiento la información

[119] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 366.

[120] Anteriormente, hemos precisado que el PLOPD 2019 ha cristalizado las mismas definiciones en la LOPD, sobre el derecho de acceso –art 13–; de rectificación –art 14–; de cancelación o eliminación –art 15–; de oposición –art 16–; a la portabilidad –art 17–; de limitación al tratamiento –art 19–; y a no ser objeto de una decisión automatizada –art 20–.

relativa a: los fines del tratamiento –art. 12.1–; la base legal que legitima el tratamiento –art. 12.2–; a los tipos de tratamiento –art. 12.3–; el tiempo de conservación –art. 12.4–; la existencia de una base de datos en donde constan sus datos–art. 12.5–; el origen de los datos, cuando no se hayan obtenido, directamente, del titular –art. 12.6–; otras finalidades y tratamientos ulteriores –art. 12.7–; la identidad y datos de contacto del responsable–art. 12.8–; la identidad y datos de contacto del delegado de protección de datos personales –art. 12.9–; las transferencias o comunicaciones nacionales e internacionales –art. 12.10–; las consecuencias para el titular de los datos personales de su entrega o negativa –art. 12.11–; el efecto de suministrar datos erróneos o inexactos –art. 12.12–; el derecho a revocar el consentimiento –art. 12.13–; los mecanismos para hacer efectivo el derecho a la portabilidad –art. 12.15–; dónde y cómo realizar sus reclamos ante el responsable y la autoridad de protección de datos –art. 12.16–; y sobre la existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles –art. 12.17–.

En este orden, entendemos que el derecho de acceso a los datos implica una obligación rigurosa de informar, en donde el principio de transparencia "debe inspirar toda la actividad de tratamiento de datos, cumpliendo, por supuesto la obligación de informar en los casos en que así se establece, como un deber de transparencia especialmente cualificado"[121]. Por ello, subrayamos que la LOPD sigue la línea que plantean, tanto los EPEI como el RGPD. Así, por ejemplo, los EPEI señalan que, mediante, el derecho de acceso "el titular tendrá el derecho de solicitar el acceso a sus datos personales que obren en posesión del responsable, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento" –art. 25.1–[122]. Y el RGPD que el

[121] Aparicio Salom, "Derechos del interesado (Arts. 12-19)", 366.

[122] En este marco, los EPEI consideran que, como parte del principio de transparencia, el responsable "informará al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto" –art. 16.1–. En este contexto, se advierte que el responsable "proporcionará al titular, al menos, la información siguiente: a. Su identidad y datos de contacto; b. Las finalidades del tratamiento a que serán sometidos sus datos personales; c. Las comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y las

interesado tendrá derecho a "obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen" –art. 15.1–[123]; en el caso de transferencias de datos, "a ser informado de las garantías adecuadas relativas a la transferencia" –art. 15.2–. Así también "facilitará una copia de los datos personales objeto de tratamiento" –art. 15.3–.

En todo caso, a diferencia del RGPD, reiteramos que la LOPD no determina que se deba facilitar una copia de los datos personales objeto de tratamiento, a pesar de la obligación contenida en el art. 12 *in fine*. Respecto a este supuesto, aplicando una interpretación que más favorezca a la efectiva vigencia del derecho a la protección de datos –un principio reconocido en el art. 10. l) de la LOPD–; en dicha Ley, la copia de los datos estaría garantizada cuando se establece que la información debe ser proporcionada al titular "por cualquier modo comprobable" –art. 12 *in fine*–. No obstante, creemos necesario que, con el objeto favorecer a la seguridad jurídica, debería incluirse en la reglamentación de la LOPD que, expresamente, el derecho de acceso del interesado comprenda que el responsable facilite una copia de los datos.

Hay que señalar que la LOPDGDD, por regla general señala que el derecho de acceso del afectado "se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679" –art. 13.1–. En todo caso, incluye las siguientes disposiciones:

finalidades que motivan la realización de las mismas; d. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad; y, e. En su caso, el origen de los datos personales cuando el responsable no los hubiere obtenido directamente del titular" –art. 16.2–.

[123] Según el RGPD, el derecho de acceso incluye la siguiente información: los fines del tratamiento –art. 15.1 a)–; las categorías de datos personales de que se trate –art. 15.1 b)–; los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales –art. 15.1 c)–; de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo –art. 15.1 d)–; la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento –art. 15.1 e)–; el derecho a presentar una reclamación ante una autoridad de control –art. 15.1 f)–; cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen –art. 15.1 g)–; la existencia de decisiones automatizadas, incluida la elaboración de perfiles, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado" –art. 15.1 h)–.

> Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.
>
> 2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.
>
> No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.
>
> 3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.
>
> 4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas[124].

De la normativa europea que se agrega, el derecho de acceso no se limita, únicamente, a garantizar el derecho a conocer los registros de información personal, que obran en la administración pública y/o privada sino también que asegura a los titulares de los datos personales algunas facultades relacionadas con la información y conocimiento de las condiciones, sobre las cuales se ejerce el tratamiento de datos. Como bien señala la CCE, el *habeas data* informativo o la dimensión utilitaria que facilita el derecho de acceso constituye "la dimensión procesal que asume el *habeas data* para recabar información acerca del qué, quién, cómo y para qué se obtuvo la información considerada personal"[125]. Por tanto, conjuntamente, con el deber de información, permite asegurar el cumplimiento del principio de transparencia en el tratamiento de los datos. De este modo, constituye una facultad que "permite el control de la propia información, al dar a conocer los datos concretos

[124] Recordemos que la LOPD 15/1999 señalaba que el derecho de acceso comprende que el titular de los datos personales o el interesado tendrá derecho a "solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos" –art. 15.1–.

[125] Véase la Resolución de la Corte Constitucional 182, Sentencia Nro. 182-15-SEP-CC –CASO Nro. 1493-10-EP– publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015.

sometidos a tratamiento, cuál es la finalidad del tratamiento, el origen de los datos y las posibles cesiones"[126].

En tanto que la legislación europea reconoce el carácter gratuito para el ejercicio de los derechos ARCO, al parecer el PLODP 2016 reconoció, únicamente, que el acceso debía realizarse en forma gratuita –art. 6.3–. Así también el PLODP 2019 señalaba que la información proporcionada al titular de los datos debía ser gratuita –art. 23–. En todo caso, a la luz del art. 12 de la LOPD, esta garantía ha sido eliminada por el legislador, sin perjuicio del reconocimiento del art. 15, sobre el ejercicio del derecho de eliminación, y del art. 29.2, sobre los derechos de los titulares de los datos crediticios. En este sentido, apreciamos que existiría una limitación en la gratuidad para el resto de facultades que posibilita el *habeas data*.

La característica de gratuidad es fundamental, por cuanto "se pretende hacer accesible su ejercicio a todos los ciudadanos, sin que la situación económica pueda ser un obstáculo para la garantía del derecho"[127]. Precisamente, en este marco, el RGPD dispone que "la información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito" –art. 12.5–. De este modo, en el RGPD, el derecho de acceso, rectificación, cancelación, oposición, portabilidad e información sobre las decisiones automatizadas tienen el carácter de gratuito[128]. No obstante, en el caso de Ecuador, habrá que tomar en consideración que, por disposición constitucional, "la persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación" –art. 92–. Naturalmente, es una garantía que, a partir del respeto del Estado constitucional de derechos y justicia, llena el vacío que ha dejado el legislador en la LOPD.

[126] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 549.
[127] Pérez-Luño Robledo, *El procedimiento de Habeas data,* 151.
[128] Al respecto, la Guía Legislativa de la OEA señala que "se debe otorgar acceso dentro de un plazo razonable, a un precio razonable, de una manera razonable y en una forma razonablemente inteligible. La carga y el costo de la presentación de los datos no deben ser irrazonables o desproporcionados".

Por una parte, el PLODP 2016 hizo referencia al derecho a "solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando exista orden de autoridad competente" –art. 6.4–. El reconocimiento de este derecho constituyó una garantía que exige que el tratamiento se cumpla, a través del respeto del consentimiento del titular y la observancia de los principios de transparencia, lealtad y licitud en el tratamiento de datos. Es decir, el derecho de solicitar prueba sobre la autorización otorgada al responsable del tratamiento. Y, por otra, además, el PLODP 2016 confundió el principio de revocación del consentimiento dentro del ejercicio de los derechos ARCO. Si bien se reconocieron los derechos a "oponerse y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales, previo el trámite legal pertinente"; esta disposición también incluyó el derecho a "revocar el consentimiento" –art. 6.5–.

Ahora bien, según los EPEI, el derecho de rectificación se plantea cuando los datos personales "resulten ser inexactos, incompletos o no se encuentren actualizados" –art. 26.1–. Asimismo, determinan que el titular de los datos personales tiene derecho a la cancelación o supresión "de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último" –art. 27.1–. De este modo, mediante el derecho de rectificación, el titular tiene el derecho a que se le corrijan los datos que resulten inexactos o incompletos, mientras que, a través del derecho de cancelación o supresión, tiene la facultad de pedir la finalización o cese del tratamiento de datos. De este modo, advertimos que el derecho de rectificación y de cancelación son "prácticamente un derecho absoluto siempre que se trate de un dato erróneo o incompleto y se aporte la documentación justificativa que muestra claramente el error o la inexactitud del dato personal o su carácter incompleto"[129].

[129] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 559. Puede decirse que, la facultad de corroborar si la información personal es actualizada y correcta se desprende del derecho de rectificación; y de la facultad de verificar si los datos personales cumplen con la finalidad que legitima su tratamiento, se desprende del derecho de cancelación de los datos personales. Cfr. Cfr. Pérez-Luño Robledo, *El procedimiento de Habeas data,* 119.

Con referencia a este aspecto, conviene precisar que la CCE ha distinguido el *habeas data* correctivo o la dimensión utilitaria que facilita el derecho de corrección orientado a "rectificar la información falsa, inexacta o imprecisa de un banco de datos"; el *habeas data* aditivo o dimensión utilitaria que permite ejercer el derecho de modificación y que "busca agregar más datos sobre aquellos que figuren en el registro respectivo, buscando actualizarlo o modificarlo según sea el caso"; y además, un *habeas data* cancelatorio cuya dimensión utilitaria permite ejercer el "derecho a la exclusión de información sensible"[130]. En este sentido, estas facultades de control y dominio de la información exigen que los datos "deberán ser exactos y estar actualizados para que en cada momento respondan con fidelidad a la situación real del sujeto. De no cumplirse esta previsión, se prevé un procedimiento de rectificación o cancelación de los mismos"[131].

El RGPD, sobre el derecho rectificación, señala que "el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan" –art. 16–; y además, reconoce el derecho de cancelación o supresión, cuando "los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo" –art. 17. a)–; "el interesado retire el consentimiento en que se basa el tratamiento*"* –art. 17. b)–; "el interesado se oponga al tratamiento" –art. 17. c)–; "los datos personales hayan sido tratados ilícitamente" –art. 17. d)–. Hasta aquí, los arts. 14 y 15 de la LOPD coinciden con el RGPD. No obstante, en dicha Ley, a diferencia del RGPD, el legislador no ha considerado la inclusión de la normativa relativa al derecho al olvido[132], una regulación que estaba incluida en el PLODP 2019[133].

[130] Véase la Resolución de la Corte Constitucional 182, Sentencia Nro. 182-15-SEP-CC –CASO Nro. 1493-10-EP– publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015.
[131] Pérez-Luño Robledo, *El procedimiento de Habeas data,* 227.
[132] Si bien en el Informe para segundo debate del Proyecto de Ley Orgánica de Protección de Datos Personales no se presentaron criterios contrarios –más bien, favorables– a su inclusión en la normativa de protección de datos; la única referencia que encontramos en dicho informe es que, en relación a los derechos de los titulares, "se ha mejorado los alcances de los siguientes derechos: información, de acceso, de oposición y portabilidad; mientras que se ha eliminado los derechos al olvido digital y de anulación". Disponible en: https://leyes.asambleanacional.gob.ec/.
[133] El art. 27 del PLODP 2019 exponía que, mediante el derecho al olvido digital, el titular tenía el derecho a "solicitar al juez competente, obtener sin dilación indebida del responsable del tratamiento, la supresión de sus datos personales que estén siendo tratados en el entorno digital".

Tomando en cuenta las disposiciones del RGPD, la LOPDGDD dispone que "el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento" –art. 14–. Así también, sobre el derecho de supresión o cancelación, reconoce que cuando "la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa" –art. 15.2–[134].

En relación al ejercicio del derecho de oposición, el PLODP 2016 reconocía a éste cuando el tratamiento de datos no cumpliera con los principios y garantías previstas para el derecho a la protección de datos –art. 6.5–. No obstante, sobre la base del art. 28 del PLODP 2019, la LOPD ha determinado que el derecho de oposición faculta al titular de los datos "a oponerse o negarse al tratamiento de sus datos personales" –art. 16–. En este marco, los EPEI consideran que este derecho procede cuando exista "una razón legítima derivada de su situación particular"; y, además, cuando "tenga por objeto la mercadotecnia directa, incluida la elaboración de perfiles, en la medida que esté relacionada con dicha actividad" –art. 28.1–. En esta línea, el RGPD reconoce que en el derecho de oposición el interesado puede oponerse en cualquier momento "por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones" –art. 21.1–. Así también el RGPD expone que cuando el tratamiento tenga por objeto la mercadotecnia directa "el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia" –art.

[134] Recordemos que la LOPD 15/1999 señalaba que el derecho de rectificación o de cancelación de los datos personales procede cuando en el tratamiento de la información "tales datos resulten inexactos o incompletos" –art. 16.2–.

21.2–[135]. Por último, la LOPDGDD regula el derecho de oposición a tenor de lo dispuesto en el RGPD. Así, se reconoce que el derecho de oposición "así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679" –art. 18–[136].

Como hemos mencionado, el PLODP 2016 no advirtió una regulación sobre los elementos o facultades que se desprenden de los derechos de rectificación, de cancelación o supresión, y oposición[137]. Mucho menos, realizó una mención sobre los derechos a la limitación del tratamiento, portabilidad de datos o decisiones individuales automatizadas. Fue, en todo caso, el PLODP 2019 el que, además, catalogó las condiciones por las cuales el titular tenía el derecho a obtener del responsable del tratamiento la limitación, portabilidad y decisiones individuales automatizadas. Naturalmente, dichas disposiciones han sido reconocidas en la LOPD.

En lo que respecta al derecho a la limitación del tratamiento, el art. 19 de la LOPD ha señalado las condiciones, por las cuales el titular tiene el derecho a la suspensión del tratamiento. Es decir, como determina el RGPD, cuando: el interesado impugne la exactitud de los datos –art. 18.1. a)–; el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso –art. 18.1. b)–; el responsable ya no necesite los datos para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la

[135] El RGPD agrega que "cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines" –art. 21.3–.

[136] Recordemos que en la LOPD 15/1999 el derecho de oposición no se regulaba como un derecho sino más bien como un supuesto dentro del principio del consentimiento. Así, esta Ley contemplaba que el afectado podía oponerse al tratamiento de sus datos personales "cuando existan motivos fundados y legítimos relativos a una concreta situación personal" –art. 6.4–.

[137] En el derecho comparado existe una amplitud al momento de definir la naturaleza del derecho de rectificación y de cancelación. Así, llamaba la atención que el PLODP 2016, únicamente, se limitara a enunciar el reconocimiento del derecho de rectificación –art. 6.1– y el derecho a la supresión o de cancelación –art. 6.5–. Si bien, enuncia por separado el derecho de eliminación o supresión y el derecho al olvido digital, destacamos que el PLODP 2019 adoptaba una regulación semejante al RGPD.

defensa de reclamaciones –art. 18.1. c)–; d) el interesado se haya opuesto al tratamiento –art. 18.1. d)–.

Sobre el derecho a la portabilidad, el art. 17 de la LOPD coincide con el RGPD, por cuanto exige como condiciones, tanto el consentimiento del titular como un tratamiento automatizado. Por último, sobre el derecho a las decisiones individuales automatizadas, también coincide con el RGPD. Si bien, el art. 20 de la LOPD reconoce el derecho a no ser objeto de decisiones basada única o parcialmente en valoración automatizadas, además, determina los casos en que no se aplica este derecho. Es decir, cuando la decisión: es necesaria para celebración o ejecución de un contrato entre el titular y el responsable –art. 20.1–; esté autorizada por la ley –art. 20.2–; esté basada en el consentimiento explícito del titular –art. 20.3–; y no conlleve impactos graves o riesgos verificables para el titular –art. 20.4–.

Bajo estas consideraciones, el ejercicio de los derechos de acceso, rectificación, cancelación u oposición constituyen, por una parte, una "herramienta constitucional con que cuenta el ciudadano para controlar el tratamiento de sus datos personales"[138]; y por otra, "deja en cabeza del ciudadano algunas facultades para exigirle al administrador de un banco de datos o archivo un tratamiento adecuado, leal y lícito de sus datos personales"[139]. Si bien uno de los principios para el efecto de la Ley es que "su ignorancia no excusa a persona alguna"; la existencia de normas dispersas, dentro del ordenamiento jurídico secundario y la falta de conocimiento de los ciudadanos y de los poderes públicos, sobre la naturaleza de estas facultades, puede repercutir en tratamientos ilícitos alejados de la finalidad para los cuales los datos personales fueron recabados. Por ello, entendíamos que "una regulación de la protección de datos sin Ley general y dependiendo de una pluralidad de normas sectoriales podría restar seguridad jurídica y hacer inefectivos los instrumentos de protección"[140].

[138] Nelson Remolina Angarita, *Derecho de Internet & Telecomunicaciones,* (Bogotá: Legis, 2003), 393.
[139] Ibíd.
[140] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 87**.**

Como señala la Guía legislativa de la OEA, la finalidad de las normas nacionales debe orientarse a que los titulares de los datos "reciban la información necesaria sobre las personas o entidades que recopilan datos, los fines para los cuales se recopilan, los mecanismos de protección conferidos a las personas y las formas en que las personas pueden ejercer esos derechos"[141]. A partir del reconocimiento de la protección de datos como un derecho fundamental, los proyectos de Ecuador estaban llamados a cumplir estas expectativas, es decir, que los titulares reciban suficiente información sobre los mecanismos de protección que –mediante el *habeas data*– se les conceda, con el objeto de ejercer las facultades de control y dominio sobre su propia información. De esta manera, "adquiere, así, relevancia una nueva situación jurídica o status que se ha venido en llamar de *habeas data*, cualificada activamente por los derechos o facultades que aseguran tal dominio"[142].

Particular importancia tiene el derecho a la información en la recogida de datos, por cuanto "constituye la base de todos los demás derechos reconocidos al interesado, ya que de otro modo será imposible que los interesados puedan ejercer derechos tales como el acceso o la oposición al tratamiento de sus datos personales"[143]. De esta manera, su garantía "no solo permite el consentimiento, sino también facilita el ejercicio del derecho de acceso, rectificación, cancelación y oposición, incluyendo la posibilidad de ejercitar estos derechos así como la identidad y dirección del responsable"[144]. Asimismo, resaltamos el derecho a revocar el consentimiento, cuando el tratamiento no cumpla con la finalidad para los cuales fueron recabados. En este caso, advertimos que "el problema estriba en que los datos pueden ser sometidos a un uso distinto de la finalidad para la cual han sido recabados, pueden

[141] La Guía Legislativa de la OEA señala además que "las normas nacionales deben asegurar que los datos personales se recopilen únicamente con fines legítimos y se procesen de una manera justa, legal y no discriminatoria (…) Deben asegurar que aquellos que recopilan, procesan, usan y difunden datos personales lo hagan de forma apropiada y con el debido respeto de los derechos de la persona".
[142] Lucas Murillo de la Cueva y Piñar Mañas, El *derecho a la autodeterminación informativa,* 18.
[143] Herrán, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, 150.
[144] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 453**.**

haberse recogido sin garantizar la información o pueden ser cedidos a terceros, de forma irregular"[145].

Por estas razones, la LOPD aprobada en mayo de 2021 debe encaminarse a garantizar el ejercicio de los derechos acceso, rectificación, cancelación, oposición, limitación al tratamiento, portabilidad y sobre decisiones automatizadas. Es fundamental el aseguramiento del derecho a ser informado, respecto del uso que se le está dando a los datos personales, pero también de revocar el consentimiento cuando en el tratamiento no se respeten sus principios, derechos y garantías constitucionales[146]. En este sentido, reconocemos que el ejercicio de las libertades y facultades que se desprenden del derecho a la protección de datos impone "la exigencia del consentimiento para el tratamiento de los datos, la obligación de ser informado y los derechos de acceso, oposición, rectificación y cancelación"[147].

Como hemos evidenciado, la comunidad internacional plantea estándares que son necesarios observarse con el objeto de asegurar una adecuada protección, no solamente en el ámbito nacional sino, además, en el contexto supranacional. Por ejemplo, el RGPD –y la misma LOPDGDD– sobre los derechos de los titulares de los datos personales garantiza: la transparencia de la información y comunicación de los datos personales; la información que deberá facilitarse cuando los datos personales se hayan o no obtenido del interesado; el derecho de acceso; el derecho de rectificación y supresión (derecho al olvido); el derecho a la limitación del tratamiento; el derecho a la portabilidad de los datos; el derecho a la oposición y a no ser objeto de una decisión basada, únicamente, en el tratamiento automatizado, incluida la elaboración de perfiles[148]. En este orden de cosas, existió una diferencia

[145] Ibíd., 135.
[146] El RGPD advierte la necesidad de garantizar "la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable" –Considerando 50–.
[147] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 135**.**
[148] El RGPD estima que "la protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se

significativa entre el PLODP 2016 y el PLODP 2019, por cuanto esta última propuesta adoptó una regulación semejante a la normativa europea y a las recomendaciones regionales que se sugieren, tanto en la Guía Legislativa de la OEA como en los EPEI. Una muestra de ello es la inclusión de derechos relativos a la portabilidad de datos, derecho a la limitación del tratamiento, derecho a no ser objeto de una decisión basada, únicamente, en valoraciones automatizadas.

Finalmente, es importante el derecho relativo a la presentación de reclamos por incumplimiento de la normativa de protección de datos, el cual se encuentra prescrito en el art.12.16 de la LOPD. Como se evidenciará en el capítulo final de este trabajo, la actividad que cumplen las Agencias o Autoridades de Protección de Datos es esencial, puesto que –a partir, de las garantías y principios que promueve el derecho a la protección de datos– estas autoridades de control y supervisión promueven "un sistema especialmente riguroso de tutela y supervisión para garantizar su efectividad, especialmente importante no solo para el derecho en sí, sino para el ejercicio y desarrollo de otros derechos"[149].

reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes" –Considerando 11–.

[149] Lucas Murillo de la Cueva y Piñar Mañas, El *derecho a la autodeterminación informativa*, 109.

## CAPÍTULO VI: OBLIGACIONES DEL RESPONSABLE Y DEL ENCARGADO DEL TRATAMIENTO

### 1. Introducción

En el objeto del derecho a la protección de datos, especial interés tienen las actividades que cumplen, tanto los responsables como los encargados del tratamiento. En la era de las tecnologías, las libertades que se protegen, a partir de este derecho se encuentran, cardinalmente, vinculadas con el respeto de la dignidad humana. Así, nos encontramos "ante la necesidad de proteger al hombre frente a las tecnologías de la información y las comunicaciones; ante la obligación de hacer presentes los derechos y tutelarnos en la era de Internet"[1]. Considerando que la garantía constitucional del *habeas data* nace con el desarrollo tecnológico, la Corte Constitucional de Ecuador advierte que aquello "obliga al funcionario que dispone la información, a presentarla cuando se requiera contar con dicha información y a explicar el uso que se hace de ella o con qué propósito la entidad tiene esa información"[2]. De esta manera, el derecho a la protección de datos, por una parte, comporta garantizar el ejercicio de las facultades de control y dominio sobre el tratamiento; y por otra, exige de los responsables del tratamiento un conjunto de medidas y acciones, que en la práctica respeten los principios y la legislación sobre protección de la información de carácter personal.

La protección de datos, no solamente es un derecho autónomo, también es un instituto de garantía de otros derechos fundamentales. Su ejercicio comprende "un haz de facultades y actuaciones de la persona que llegaría a significar la posibilidad para la persona de delimitar y determinar hasta qué punto desea comunicar y compartir sus datos"[3]. Por tanto, motiva a la observancia de una serie de principios

[1] Antonio Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, (Valencia: Tirant lo Blanch, 2010), 33.
[2] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-09-SEP-CC –CASO Nro. 14-9-EP– publicada en el Registro Oficial Nro.18 de 3 de septiembre de 2009.
[3] Ana Isabel Herrán, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, (Madrid: Dykinson, 2002), 114.

que los responsables y encargados del tratamiento deben aplicar, con el objeto de que "puedan cumplir de manera satisfactoria las exigencias jurídicas y de responsabilidad social empresarial vinculadas a las nuevas exigencias y requerimientos derivados de la protección de datos de carácter personal"[4].

No obstante, la administración ha demostrado que "no tiene, en general, hábito en la aplicación de la responsabilidad proactiva (cabe recordar que es un término/concepto anglosajón) como piedra angular de sus actuaciones, y en particular, en lo relativo a la protección de datos de carácter personal"[5]. Desde esta perspectiva, las obligaciones que se desprenden de los principios que integran este derecho fundamental precisan un examen especial, puesto que, la protección de datos "si bien tiene como beneficiario directo a la persona interesada, no afecta sólo al sujeto individual sino a toda la sociedad en su conjunto"[6]. En todo caso, no está por demás insistir en que, en el tratamiento de la información, "los obligados del derecho a la protección de datos personales ya no son sólo los poderes públicos sino también los particulares y, en especial, las empresas que se encargan de gestionar bancos de datos personales"[7].

Ahora bien, habiendo señalado que la protección integral de este derecho implica la observancia de una serie de principios, cuyo fin es garantizar la seguridad jurídica; la observancia de estos principios –que conlleva, implícitamente, el respeto de ciertas obligaciones– derivan en el cumplimiento de mecanismos de protección que los responsables y encargados del tratamiento deben aplicar a la hora de utilizar los datos personales. Aunque, el cumplimiento de estos principios podría catalogarse como obligaciones de los responsables y encargados, subrayamos que las reglas y normas que regulan el tratamiento de datos "tienen un alcance y trascendencia de

[4] Javier Puyol Montero, "Los principios del Derecho a la Protección de Datos", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 136.
[5] Raúl Costa Hernandis, "Responsabilidad del responsable del tratamiento (Art. 24)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 420.
[6] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 39**.**
[7] Mónica Arenas Ramiro, "La protección de datos personales en los países de la Unión Europea", *Revista Jurídica de Castilla y León*, Nro. 16 (2008):113-168.

mayor envergadura, puesto que no solamente afectan al responsable del tratamiento, sino a todas aquellas personas físicas o jurídicas que intervienen en el tratamiento de datos"[8].

A partir de las bases del Estado constitucional de derechos y justicia en Ecuador, la tutela efectiva del derecho a la protección de datos significa una de las cuestiones más importantes que debe abordarse. En términos de definir las obligaciones que plantea este derecho, no debe olvidarse que dentro de este modelo constitucional "el Estado es un medio que tiene como fin la realización y la protección de los derechos"[9]. Por tanto, a los responsables y encargados –en el ámbito público y privado– se les exige que el tratamiento debe responder a la realización del derecho a la protección de datos, el cual se encuentra reconocido en el ordenamiento constitucional. En todo caso, considerando la aprobación de la Ley Orgánica de Protección de Datos Personales en mayo de 2021, este capítulo se orienta a estudiar las obligaciones del responsable y encargado del tratamiento. Para este fin, los proyectos de Ley en Ecuador de 2016 y 2019 constituyen una base referencial, para el análisis de las principales obligaciones, que deben cumplir las personas que llevan a cabo actividades u operaciones relacionadas con el tratamiento. Lógicamente, la Guía Legislativa de la OEA, los Estándares de protección de datos personales para los Estados Iberoamericanos, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales serán los principales instrumentos regionales que nos permitirán determinar las obligaciones que deben establecerse para los responsables y encargados.

[8] Puyol Montero, "Los principios del Derecho a la Protección de Datos", 136.
[9] Ramiro Ávila Santamaría, *El Neoconstitucionalismo andino,* (Quito-Ecuador: Universidad Andina Simón Bolívar, 2016), 57.

## 2. Obligaciones del responsable del tratamiento

En el contexto ecuatoriano, las obligaciones dentro del tratamiento de la información nacen de conformidad al mandato constitucional, dispuesto en el inciso final del art. 92 para la garantía del *habeas data*. Por una parte, se determina que los responsables del tratamiento "podrán difundir la información archivada con autorización de su titular o de la Ley"; y por otra que, además, "en el caso de datos sensibles, cuyo archivo deberá estar autorizado por la Ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias". Todo ello, sin perjuicio de garantizar que el titular de los datos pueda "solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación". Naturalmente, habiéndose aprobado la Ley Orgánica de Protección de Datos Personales –en adelante LOPD– se establece un régimen jurídico en donde a los responsables y encargados se les exige el cumplimiento de una serie de garantías y obligaciones frente al tratamiento de datos personales.

Entre las principales obligaciones se destacan: cumplir sus actividades de tratamiento, respetando la legislación y el consentimiento y/o autorización prestado por el titular de los datos; garantizar el ejercicio de los derechos de acceso, rectificación, cancelación u oposición; y adoptar medidas de seguridad en el tratamiento de los datos sensibles. En todo caso, estas obligaciones que nacen de la garantía del *habeas data,* no pueden considerarse como las únicas y necesarias para regular el tratamiento de datos personales. Hoy en día, la responsabilidad del responsable va más allá. No solamente debe cumplir con la legislación, sino vigilar y demostrar, permanentemente, por que ésta se cumpla.

Asumiendo que el derecho a la protección de datos responde a las potenciales intromisiones ilegítimas que pueden resultar, tanto en la sociedad de la información como en la economía digital, la garantía de la seguridad jurídica y la transparencia en el tratamiento de la información exige adoptar un marco de supervisión y control que –aplicable a los responsables y encargados– sea coherente con el objeto que

persigue este derecho fundamental[10]. Por ello, atendiendo al principio de responsabilidad proactiva, el responsable coadyuva a este objetivo, mediante la adopción de medidas apropiadas, que garanticen y acrediten el cumplimiento de los principios de la protección de datos.

> Se pasa así de un modelo reactivo a un modelo preventivo, que exige de los responsables de tratamiento conocer el derecho fundamental (el grado de conocimiento exigido será mayor cuanto mayor sea el volumen de los datos objeto del tratamiento o los datos afectados sean más sensibles) y una reflexión previa sobre la afectación a la privacidad de los tratamientos previstos. Los cambios que se introducen como consecuencia de la aplicación de este principio se observan ya desde las fases iniciales del tratamiento de los datos, pudiendo citarse los siguientes ejemplos: desaparición del registro de ficheros, obligación de realizar análisis de riesgos y evaluaciones de impacto en determinados tratamientos, o la obligatoriedad de asumir la privacidad por diseño y por defecto[11].

Bajo estas consideraciones, "si bien habitualmente se hace referencia al derecho a la intimidad, en puridad jurídica también se alude a la obligación que los demás, terceros ajenos a la esfera personal de cada individuo deben asumir"[12]. En el contexto del tratamiento de la información, la protección de la intimidad y de otros bienes jurídicos se presenta "no sólo como un derecho, sino como el deber de respetar un ámbito propio y esencial de cada persona que afecta al resto de individuos, con la aspiración de que dicho ámbito quede al margen de la indiscreción ajena en tanto que es la propia persona quien lo determina"[13].

### 2.1 Obligaciones generales

[10] Como señala el RGPD, "para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros" –Considerando 13–.

[11] Ana Aperribai Ulacia y Román Intxaurtieta Madariaga, "Consideraciones de la Agencia Vasca de Protección de Datos", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 100.

[12] Herrán, *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*, (Madrid: Dykinson, 2002), 27.

[13] Ibíd.

La Corte Constitucional de Ecuador –en adelante CCE– destaca que el tratamiento de la información debe "garantizar, sin discriminación alguna, el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales"[14]. Así también según lo previsto en la LOPD, la normativa de protección de datos aplicable a este derecho fundamental "no podrá limitar el ejercicio de los derechos –art. 6–, la cual, además, deberá dar cumplimiento "a los estándares internacionales en materia de derechos humanos" –art. 11–. Al constituirse la protección de datos, como un derecho global que afecta a toda la sociedad, a partir del desarrollo del fenómeno tecnológico, las nuevas generaciones de derechos "se hallan aunados entre sí por su incidencia universal en la vida de todos los hombres y exigen para su realización la comunidad de esfuerzos y responsabilidades a escala planetaria"[15]. De esta manera, nos encontramos frente a un nuevo marco de protección de datos, en donde, además, se deja a juicio de los responsables del tratamiento "la adopción de las medidas tanto técnicas como organizativas que entienda necesarias para garantizar el cumplimiento del principio de integridad de los datos"[16].

En el ámbito internacional, los ordenamientos jurídicos coinciden en que las obligaciones que se derivan del tratamiento reflejan la necesidad de establecer un respeto integral sobre los principios y exigencias, que demanda la protección de este derecho fundamental[17]. En este punto, se advierte la obligación de adoptar

[14] Véase la Resolución de la Corte Constitucional 19, Sentencia Nro. 19-9-SEP-CC –CASO Nro. 14-9-EP– publicada en el Registro Oficial Nro. 18 de 3 de septiembre de 2009. Como hemos señalado en otro momento, la CCE destaca la importancia del respeto de los principios y garantías previstas para la protección de datos, por parte de los responsables del tratamiento, señalando que "corresponde también un manejo responsable de la misma, debido a que cualquier acción u omisión en su tratamiento por parte de los servidores públicos responsables puede generar una violación a derechos fundamentales de las personas".

[15] Antonio Pérez Luño, *Derechos Humanos, Estado de Derecho y Constitución*, (Madrid: Tecnos, 2010), 373-374.

[16] Aperribai Ulacia e Intxaurtieta Madariaga, "Consideraciones de la Agencia Vasca de Protección de Datos", 102.

[17] Recordemos que los EPEI señalan la necesidad de adoptar medidas preventivas que "permitan al responsable responder proactivamente ante los posibles problemas relacionados con el derecho a la protección de datos personales como son la adopción de esquemas de autorregulación vinculante o sistemas de certificación en la materia; la designación de un oficial de protección de datos personales; la elaboración de evaluaciones de impacto a la protección de datos personales y la privacidad por defecto y por diseño, entre otras, lo cual resulta esencial en el ámbito de las tecnologías de la información y las telecomunicaciones" –Considerando 23–. Así también el RGPD

medidas proactivas, técnicas y organizativas, a través de esquemas de autorregulación y evaluaciones de impacto, que permitan al responsable del tratamiento mejorar los elementos de seguridad, y, en suma, garantizar el cumplimiento de los principios previstos para la protección de datos. Naturalmente, según dispone la LOPD, dichas obligaciones deben observar los principios del ordenamiento jurídico de protección de datos "y como mínimo a los criterios de legalidad, proporcionalidad y necesidad" –art. 11–. De este modo, "se refuerzan también las garantías de los titulares de los datos personales frente a nuevas formas de agresión a los equipos informáticos que pudieran redundar en una vulneración de los datos que les conciernen"[18].

En este marco, sin duda, un ejemplo constituye las disposiciones del RGPD, por cuanto "pretende hacer más sencilla la protección de datos, reduciendo las cargas administrativas para las empresas, al mismo tiempo que se incrementa la *accountability*"[19]. En efecto, el Reglamento elimina la notificación de los tratamientos e introduce, por primera vez, el principio de responsabilidad proactiva[20], el cual exige de los responsables del tratamiento tutelar y contribuir a la supervisión de la legislación de protección datos, "con iniciativa, diligente, que no se limita a cumplir una norma porque la solución no a venir definida en ésta"[21]. Es decir, se pretende

enfatiza el rol que cumplen los responsables del tratamiento, señalando que "la protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad" –Considerando 78–.

[18] Enrique Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías*, (Madrid: Editorial Dykinson S.L, 2017), 248.

[19] Antonio Troncoso, "Autoridades de Control Independientes", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 463.

[20] Respecto al principio de responsabilidad, recordemos que este nace también de los EPEI como un principio para el tratamiento de la información, por el cual, el responsable "implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones" –art. 20.1–, y deberá revisar y evaluar "permanentemente los mecanismos que para tal afecto adopte voluntariamente para cumplir con el principio de responsabilidad" –art. 20.4–.

[21] Troncoso, "Autoridades de Control Independientes", 465.

que el marco de protección de datos personales, no solamente se ampare en disposiciones legales sino también en las medidas que los responsables puedan adoptar de manera proactiva. Se concibe, así una visión integral, en donde la supervisión y la tutela del derecho a la protección de datos, no corresponde, únicamente, a las autoridades de control, sino a los responsables del tratamiento.

Por ejemplo, los EPEI consideran que –con el objeto de dar cuenta del principio de responsabilidad en la protección de datos–, el responsable se encuentra obliga a: "destinar recursos para la instrumentación de programas y políticas de protección de datos" –art. 20.3 a)–; "implementar sistemas de administración de riesgos asociados al tratamiento" –art. 20.3 b)–; "elaborar políticas y programas de protección de datos obligatorios y exigibles al interior de la organización del responsable" –art. 20.3 c)–; "poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos" –art. 20.3 d)–; "revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran" –art. 20.3 e)–; "establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos" –art. 20.3 f)–; y "establecer procedimientos para recibir y responder dudas y quejas de los titulares" –art. 20.3 g)–.

Del mismo modo, tomando en consideración la naturaleza, el ámbito, los fines del tratamiento y los riesgos que supone éste en la era digital, el RGPD señala que el responsable "aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario" –art. 24.1–[22], incluyendo la aplicación de "oportunas políticas de protección de datos"

[22] Respecto a la revisión y actualización de las medidas técnicas y organizativas, los EPEI precisan que el objeto de estas medidas es "medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable" –art. 20.4–.

–art. 24.2–[23]. Además, de la adhesión a códigos de conducta[24], o a un mecanismo de certificación–art. 24.3–[25]. Asimismo, atendiendo a las disposiciones del RGPD, la LOPDGDD establece que, tanto los responsables como encargados con el objeto de garantizar y acreditar que el tratamiento respete la normativa de protección de datos "determinarán las medidas técnicas y organizativas apropiadas (…) valorarán si procede la realización de la evaluación de impacto en la protección de datos y la consulta previa" –art. 28.1–.

Ahora bien, el PLODP 2016, de modo general, dispuso que se debían "respetar en todo momento los principios generales de la protección de datos personales" –art. 8.3–. Esta propuesta no prescribía la obligación de considerar medidas técnicas y organizativas que garanticen y demuestren, que el tratamiento se cumpliera conforme a la normativa de protección de datos; y así también no anticipó que dichas medidas fueran revisadas y actualizadas. En todo caso, si bien evidenciamos estas omisiones en dicha propuesta, corresponde advertir que, "la decisión sobre los medios a emplear en el tratamiento de los datos no reside ya (al menos en lo

[23] El RGPD define como normas corporativas vinculantes a "las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta" –art. 4.20–.

[24] El RGPD determina que "se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas" –Considerando 98–. En este mismo sentido, la Guía Legislativa de la OEA señala que se deben "crear medios razonables para que las personas ejerzan sus derechos y fomentar y apoyar la autorregulación (con códigos de conducta o por otros medios) de los controladores de datos y los procesadores de datos".

[25] El RGPD agrega que la adhesión a un código de conducta aprobado, o a un mecanismo de certificación aprobado "puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable" –Considerando 81–. Así también los EPEI apuntan que los responsables del tratamiento podrán adherirse a mecanismos de autorregulación, para demostrar el cumplimiento de la legislación de protección de datos, por lo que "se podrán desarrollar, entre otros, códigos deontológicos y sistemas de certificación y sus respectivos sellos de confianza" –art. 40.2–.

referente a las medidas de seguridad) en el legislador, sino que es el propio responsable quien debe determinar estos aspectos"[26].

No obstante, a la luz del art. 71 del PLODP 2019, la LOPD ha concretado la necesidad de aplicar e implementar requisitos y herramientas técnicas, jurídicas, administrativas y organizativas apropiadas, "a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente Ley" –art. 47.2–; y además, que el responsable debe "aplicar e implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas " –art. 47.3–. En este sentido, destacamos que la LOPD sigue la línea del RGPD, por cuanto cambia el paradigma "de acción-reacción o, mejor dicho, de nivel de sensibilidad de la información, igual a, conocimiento de las medidas concretas a aplicar (…) lo cual desde el punto de vista práctico supondrá la atención proporcionada, periódica y continuada de las citadas medidas"[27].

Por otra parte, el PLODP 2016 tampoco prescribió la obligación de aplicar políticas de protección de datos o normas corporativas vinculantes; ni, a su vez, la obligación de adherirse a códigos de conducta o mecanismos de certificación, para demostrar el cumplimiento de las obligaciones del responsable. En este punto, advertimos que, tanto las políticas o normas corporativas vinculantes como los códigos de conducta o mecanismos de certificación, tienen el objeto de constituirse como medidas preventivas de protección de datos y de satisfacción del principio de responsabilidad proactiva. Por el contrario, el art. 71 del PLODP 2019 introdujo en la LOPD que el responsable debe "implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso particular" –art. 47.4–[28], las cuales,

[26] Aperribai Ulacia e Intxaurtieta Madariaga, "Consideraciones de la Agencia Vasca de Protección de Datos", 102.
[27] Costa Hernandis, "Responsabilidad del responsable del tratamiento (Art. 24)", 421.
[28] En todo caso, el PLODP 2019 reconoce que los responsables o encargados del tratamiento "podrán presentar a la Autoridad de Protección de Datos Personales normas corporativas vinculantes, específicas y aplicadas al ámbito de su actividad" –art. 68–.

"desde el punto de vista práctico se traducirán en la creación de las directrices que permitan el conocimiento de la organización respecto al tratamiento de los datos personales tratados"[29]. En consecuencia, al igual que en el marco europeo, distinguimos "un nuevo escenario para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable, especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo"[30].

En este punto, conviene señalar que el del PLODP 2019 establecía como una obligación "adherirse a códigos de protección, mecanismos de certificación o sellos de protección de datos personales aprobados por la Autoridad de Protección de Datos" –art. 71.5–. Sin embargo, en la LOPD el legislador ha considerado excluirla de las obligaciones del responsable, por cuanto asumió que "no debe ser un rol de la Autoridad de Protección de Datos, ni del Estado, regular estos mecanismos de certificación. Adicionalmente, las Entidades Certificadoras y los sellos que deben emitir, generarían una carga operativa innecesaria para la Autoridad de Control y un trámite adicional para los proveedores y usuarios"[31]. En todo caso, como parte del desarrollo normativo del principio de responsabilidad proactiva, la LOPD contempla un esquema de autorregulación para los responsables y encargados del

[29] Costa Hernandis, "Responsabilidad del responsable del tratamiento (Art. 24)", 422.
[30] Ibíd., 424.
[31] Dichas consideraciones formaron parte del Informe para segundo debate del Proyecto de Ley Orgánica de Protección de Datos Personales. Disponible en: https://leyes.asambleanacional.gob.ec/. En todo caso, valga la oportunidad considerar que, la elaboración de códigos de conducta supone "una pluralidad de contenidos con relación al ámbito de la privacidad, pero sin lugar a dudas, uno de sus principales componentes los será la determinación de aquellas obligaciones que han de asumir tanto los responsables como los encargados de los tratamientos, y al mismo tiempo, el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento". Así también respecto a la obtención de certificaciones "debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a las personas cuyos datos estén siendo objeto de tratamiento, poder evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes". Cfr. Javier Puyol Montero, "El Reglamento General de Protección de Datos, y la *Pymes*", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 156-158.

tratamiento, sobre la base de los códigos de conducta, certificaciones, sellos y marcas de protección –art. 52–.

Por otra parte, tanto el responsable como el encargado del tratamiento, deben cooperar con las autoridades de control de datos, con el objeto de procurar una mejor garantía del derecho a la protección de datos y demostrar transparencia, en el tratamiento de la información[32]. Por ejemplo, el RGPD dispone que aquellos "y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones" –art. 31–. Así pues, se pone de manifiesto que:

> El responsable y el encargado de tratamiento, así como, en su caso, sus representantes, deben tener en cuenta que la protección de datos es un derecho fundamental a respetar en todas las etapas de cualquier actividad de tratamiento de datos personales, evaluando los riesgos para los derechos y libertades de las personas titulares de los datos y adoptando las medidas adecuadas para minimizarlos. En todo caso, será fundamental que exista cooperación entre todos aquellos agentes que intervienen en el diseño y creación de un sistema de información y en la cadena de fases posteriores ligadas al ciclo de vida de los datos personales, para poder demostrar, la responsabilidad en el cumplimiento[33].

Con referencia a este aspecto, a partir del art. 71 del PLODP 2019, la LOPD pone de manifiesto que una de las obligaciones que deben cumplir los responsables del tratamiento es el tratamiento de datos "en estricto apego a los lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales" –art. 47.1–; la garantía e implementación de medidas previstas en los "los lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales" –art. 47.2–; y la contribución a "la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales" –art. 47.14–. Si bien la LOPD, no prescribe una norma que exija la cooperación con las autoridades de control, advertimos que de las disposiciones que se anotan se deriva que, al menos el responsable del tratamiento, debe contribuir y cooperar con la

[32] El RGPD advierte que, "para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad. Todos los responsables y encargados están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento" –Considerando 82–.

[33] María José Blanco Antón, "Cooperación con la autoridad de control (Art. 31)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 451.

autoridad de control en el objetivo de garantizar el cumplimiento de la legislación de protección de datos, sobre la base de "un modelo proactivo en el que es necesario demostrar la actitud responsable con el cumplimiento de todos los actores que intervienen en el tratamiento de datos personales"[34].

### 2.2 Protección de datos, desde el diseño y por defecto

Estas obligaciones generales que corresponden a los responsable del tratamiento, "tanto en uno y otro caso, lo que está planteando el legislador europeo es una actitud que los responsables de tratamiento deben tener en relación con las operaciones de tratamiento de su responsabilidad"[35]. Naturalmente, esta obligación o actitud del responsable, desde el diseño y por defecto, tiene por objeto garantizar, por una parte, el cumplimiento de los requisitos y principios de la normativa de protección de datos y, por otra, demostrar el respeto de las libertades de los interesados o titulares del derecho a la protección de datos. Desde esta perspectiva, "se exige una responsabilidad proactiva, en lugar de la responsabilidad reactiva (enfoque basado en riesgos), debiéndose actuar con carácter preventivo, tener la diligencia debida para evitar tratamientos o incumplimientos no deseados en la protección de los intereses de los ciudadanos en el ámbito de su privacidad"[36].

En relación a la protección de datos, desde el diseño, el RGPD señala que, el responsable del tratamiento, teniendo en cuenta "el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas", aplicará, al momento de determinar los medios del tratamiento, y al momento mismo de este, "medidas técnicas y

[34] Blanco Antón, "Cooperación con la autoridad de control (Art. 31)", 451.
[35] Ramón Miralles López, "Protección de datos desde el diseño y por defecto (Art. 25)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 427.
[36] Juan Carlos Bajo, "Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el *compliance*", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 281.

organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento"[37] –art. 25.1–. En tal sentido, esta obligación "tiene que ver con la prevención, de modo que antes de iniciar las operaciones de tratamiento, es decir, en el momento en que se están definiendo cómo serán los medios de tratamiento, pero también al implantar y operar los tratamientos, se tengan en cuenta las exigencias que se derivan de la regulación respecto de los principios, derechos y obligaciones"[38]

Ahora bien, con referencia a la protección de datos, por defecto, el RGPD dispone que, el responsable considerará que, la aplicación de las medidas técnicas y organizativas garanticen que "por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento" –art. 25.2–[39]. Así, esta obligación "implica implantar las operaciones de tratamiento teniendo en cuenta algunas cuestiones concretas que garanticen, desde el momento del inicio de los tratamientos, que estos se van a tratar teniendo en cuenta requisitos previstos en el Reglamento"[40].

Por último, para demostrar el cumplimiento de estas obligaciones, el RGPD añade que "podrá utilizarse un mecanismo de certificación" –art. 25.3–. Por tanto, basándonos en estos tres presupuestos:

> Lo que pretende el legislador es forzar un cambio de actitud, ya que, frecuentemente, la necesidad de adecuarse a las obligaciones previstas en la legislación que regula el derecho fundamental a la protección de los datos de carácter personal, se considera una barrera para la consecución de los objetivos de una iniciativa, proyecto, negocio, servicio, tecnología, etc.

[37] En este caso, el RGPD señala que "al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos" –Considerando 78–.

[38] Miralles López, "Protección de datos desde el diseño y por defecto (Art. 25)", 427.

[39] Al respecto, el RGPD agrega que "esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

[40] Miralles López, "Protección de datos desde el diseño y por defecto (Art. 25)", 427

> que precisa del tratamiento de datos de carácter personal para su desarrollo. No solo la adecuación a las obligaciones, también los principios y derechos que configuran el derecho a la protección de los datos de carácter personal se perciben como un conjunto de trabas y dificultades[41].

En este marco, no está por demás señalar que la LOPDGDD también obliga a los responsables y encargados del tratamiento a aplicar las medidas técnicas y organizativas apropiadas derivadas de la protección de datos, desde el diseño y por defecto –art. 28.1–, en donde, "el objetivo final de la implantación de dichas políticas o medidas de protección de datos o programas de gestión interna de la privacidad no es otro que garantizar que las actividades de tratamiento realizadas por el responsable cumplen con lo establecido en el Reglamento"[42]. Bajo estas precisiones que corresponden a la protección de datos, desde el diseño y por defecto, lo cual incluye el uso de mecanismos de certificación para demostrar su cumplimiento; el PLODP 2016 omitió señalar estas obligaciones que, como hemos destacado, garantizan y demuestran que "el tratamiento es adecuado conforme al ámbito, al contexto y a los fines del tratamiento, así como una adecuada gestión de riesgos en el tratamiento de los datos que puedan afectar a los derechos y libertades de las personas físicas"[43]. A la luz del art. 71 del PLODP 2019, la LOPD ha materializado que, solamente, los responsables del tratamiento deberán "implementar la protección de datos personales desde el diseño y por defecto" –art. 47.9–.

Inicialmente, el art. 52 del PLODP 2019 determinó que la protección de datos personales, desde el diseño y por defecto, implicaba que el responsable y el encargado establecerían "medidas técnicas, organizativas y de cualquier otra índole con miras a garantizar que los procesos y medios de tratamiento protejan los datos personales desde su diseño, así como sus configuraciones se encuentren por defecto en cumplimiento de la presente Ley" –art. 52–. Así, a diferencia del RGPD, llamaba la atención que el PLODP 2019 no distinguiera, claramente, la prevención que –desde el diseño– debe existir antes de iniciar el tratamiento, con la

[41] Ibíd.
[42] Bajo, "Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el *compliance*", 280.
[43] Ibíd., 281

implantación –desde el defecto– de medidas técnicas y organizativas que garanticen que, desde el inicio del tratamiento, los datos personales sean los necesarios, conforme a los fines para los cuales fueron recabados.

En todo caso, si bien, por un lado, "la obligatoriedad de estas medidas, o el modo en que se apliquen, dependerán de factores que habrá que tener en cuenta en cada caso, como el tipo de tratamiento y el riesgo que dicho tratamiento implica para los derechos y libertades de los interesados"[44]; y por otro, estarán supeditadas a un modelo proactivo, en el que se deberá demostrar el cumplimiento de la legislación de protección de datos. Apreciamos que, finalmente, el legislador ha aclarado en la LOPD que la protección de datos desde el diseño constituye un deber del responsable "de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento" –art. 39–; en tanto que, la protección de datos por defecto tiene relación con que el responsable "debe aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento" –art. 39–.

Hay que recordar también que el art. 71.5 del PLODP 2019 permitía a los responsables adherirse a mecanismos de certificación o sellos de protección de datos, con el objeto de acreditar el cumplimiento de sus obligaciones. Como hemos señalado, si bien esta obligación ya no forma parte de los deberes del responsable, dispuestos en el art. 47 de la LOPD[45], conviene advertir que, dicha disposición proporcionaba a los responsables un importante instrumento para que éstos puedan

[44] Ibíd.

[45] Dentro del Informe para segundo debate del Proyecto de Ley Orgánica de Protección de Datos Personales, otra de las razones por las que el legislador ha considerado excluir, dichos instrumentos, de las obligaciones del responsable es que, "las Entidades Certificadoras no existen en la mayor parte de los estándares internacionales y en los casos que han sido previstas, no se han implementado o están en desuso, lo que provocaría riesgos de incompatibilidad con los marcos normativos de otras jurisdicciones importantes, por lo que dentro del proyecto del proyecto de Ley se contemplan como mecanismos de autorregulación que garanticen un doble seguro en la protección de los datos personales". Disponible en: https://leyes.asambleanacional.gob.ec/.

demostrar el cumplimiento de la protección de datos, desde el diseño y por defecto, por cuanto, "estos son cada vez más exigentes y en muchas ocasiones solicitan contratar exclusivamente con proveedores certificados, a los efectos de obtener unas mayores garantías jurídicas en el tratamiento de los datos de carácter personal" [46]. De esta manera, según la LOPD se invoca un deber voluntario, mas no obligatorio, que se adecua al principio de responsabilidad proactiva del responsable del tratamiento.

Finalmente, debemos apuntar que los EPEI consideran como medidas proactivas en el tratamiento de datos a la privacidad por diseño y privacidad por defecto. Así, este instrumento prescribe que el responsable del tratamiento aplicará, desde el diseño, "medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional" –art. 38.1–; y que, también garantizará que "sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación" –art. 38.2–. En este orden, además, la Guía Legislativa de la OEA advierte de la necesidad de incorporar "la protección de la privacidad en el diseño y la arquitectura de sus sistemas de tecnología de la información y en sus prácticas comerciales"[47]. Por ello, consideramos que estas obligaciones son fundamentales, por cuanto:

> Representa un rasgo novedoso de la nueva normativa en su propósito de garantizar que el responsable del tratamiento de datos personales responda de la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema de información para resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos[48].

[46] Puyol Montero, "El Reglamento General de Protección de Datos, y la *Pymes*", 158.

[47] En todo caso, la Guía Legislativa de la OEA agrega que "deben incorporarse consideraciones de privacidad y seguridad en cada etapa del diseño de los productos. Los controladores de datos deben estar preparados para demostrar sus programas de gestión de la privacidad cuando se lo solicite, en particular a petición de una autoridad competente a cargo de la aplicación de la normativa en materia de privacidad o de otra entidad que se encargue de promover la adhesión a un código de conducta".

[48] Pérez-Luño Robledo, *El procedimiento de Habeas data,* 248.

Otras obligaciones importantes que se atribuyen a los responsables del tratamiento son: la garantía de la seguridad del tratamiento, la evaluación de impacto relativa a la protección de datos y la consulta previa[49]. Sin haber existido, en este ámbito, disposiciones relacionadas en el PLODP 2016, destacamos que el PLODP 2019 sí hizo referencia a estas obligaciones, las cuales se encuentran reconocidas en el actual marco normativo de la LOPD.

### 2.3 Seguridad de los datos personales

Basándose en el art. 50 del PLODP 2019, la LOPD ha concretado que el responsable o encargado del tratamiento, con sujeción al principio de seguridad de datos –art. 10. j)–, deberá "tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento" –art. 37–[50]. En este sentido, como parte de las obligaciones de los responsables, la LOPD determina que deberá "tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y vulneraciones identificadas" –art. 47.7–.

[49] El RGPD, sobre las evaluaciones de impacto señala que "a fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo" –Considerando 84–. Así también, sobre la consulta previa, el RGPD determina que "debe consultarse a la autoridad de control antes de iniciar las actividades de tratamiento si una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación" –Considerando 94–.

[50] En este aspecto, el RGPD precisa que "a fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse" –Considerando 83–.

Estas prescripciones guardan relación con lo dispuesto por el RGPD, por cuanto señala que, tomando en cuenta los costos, el estado de la técnica, la naturaleza, alcance, contexto y los fines del tratamiento, "el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo" –art. 32.1–. Si bien, "la seguridad de la información no es un estado que se pueda alcanzar, sino que es un proceso de adaptación y mejora continua que debe mantenerse y repetirse con la adecuada regularidad en el tiempo"[51], esta obligación conlleva "realizar una evaluación de riegos, que permita adoptar medidas para proteger los datos contra su destrucción accidental o ilícita, pérdida accidental o cualquier tratamiento ilícito como la comunicación, difusión, el acceso no autorizado o la alteración de los datos personales"[52].

Corresponde advertir que, además, la LOPD coincide con el RGPD sobre las medidas técnicas y organizativas que deben adoptarse para demostrar y garantizar un nivel de seguridad adecuado, frente a los riesgos identificados. Así, por ejemplo, reiteramos que el art. 37 de la LOPD señala medidas de: "confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios de tratamiento de datos personales, de forma rápida en caso de incidente"; "resiliencia técnica, física, administrativa y jurídica"; y "anonimización, seudonimización o cifrado de datos personales"[53]. Ahora bien, el RGPD añade que "al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el

[51] Ignacio González Ubierna, "Seguridad del tratamiento (Art. 32)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 455.

[52] Antonio Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", *Revista Española de Derecho Europeo*, Nro. 43 (2012): 25-184.

[53] Frente a esta última medida, reiteramos la importancia de distinguir los conceptos de anonimización y seudonimización. Como hemos precisado en otro momento, para que opere el derecho a la protección de datos debe existir un tratamiento y que, en efecto, este se sustancie sobre información personal. La anonimización constituye un procedimiento de disociación absoluta o definitiva, el cual impediría la identificación del titular de los datos y, por tanto, supondría la imposibilidad de que exista un tratamiento. Desde esta perspectiva, lo correcto sería que la LOPD considere a la seudonimización como una medida de seguridad, por cuanto –al tenor del RGPD– los datos seudonimizados pueden ser atribuidos a una persona, por medio del uso de información adicional.

tratamiento de datos" –art. 32.2–. Esta medida, también se encuentra recogida en la LOPD, por cuanto se señala que, al momento de implementar las medidas de seguridad de la información personal, se deberá "identificar la probabilidad de riesgos" –art. 37–. Así pues, "para seleccionar las medidas de seguridad adecuadas, debemos basarnos en los riesgos para las personas físicas, así como en lo que es razonable y técnicamente posible"[54]. Por ello, resaltamos que este enfoque "implica tener en cuenta el riesgo del tratamiento para los derechos y libertades de las personas. De manera que sólo cuando haya un riesgo alto para esos derechos y libertades se aplicarán ciertas medidas"[55].

Por otra parte, dentro de esta obligación, el RGPD determina "la adhesión a un código de conducta aprobado o a un mecanismo de certificación" –art. 32.3–, como un elemento para demostrar el cumplimiento de la legislación de protección de datos. Frente a este supuesto, la LOPD precisa, además, que los responsables y encargados podrán implementar "acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta" –art. 37.4–, reconocidos y autorizados por la autoridad de control. De esta forma, manifestamos que los códigos de conducta y, en suma, los mecanismos de certificación constituyen instrumentos que garantizan la confianza "y el aumento de la transparencia y la reputación frente a terceros y el propio regulador, a consecuencia de la tenencia y el reconocimiento de la misma"[56].

Por último, el RGPD apunta que el responsable y el encargado "tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable" –art. 32.4–. En este orden, la LOPD sigue esta línea, advirtiendo que el responsable suscribirá "contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del

[54] González Ubierna, "Seguridad del tratamiento (Art. 32)", 454.
[55] Bajo, "Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el *compliance*", 280.
[56] Puyol Montero, "El Reglamento General de Protección de Datos, y la *Pymes*", 160.

tratamiento de datos personales o que tenga conocimiento de los datos personales" –art. 47.10–. A partir de esta disposición, entendemos que, a todos los involucrados en el tratamiento se les exige "una actitud previa, consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo"[57]. De este modo, además, debe advertirse que la LOPD recoge, igualmente, las prescripciones de los EPEI, sobre el principio de seguridad en el tratamiento de datos, por cuanto este instrumento señala que el responsable "establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales" –art. 21.1–[58].

Bajo estas consideraciones, concluimos que, frente al tratamiento de datos se deben aplicar "medidas de seguridad a los sistemas de información que los tratan –además de la confidencialidad, en sentido estricto, también con relación a la disponibilidad, la integridad y la autenticidad–, con objeto de evitar fugas incontroladas de datos personales"[59]. Si bien las garantías de seguridad son fundamentales a la hora de enfrentar las amenazas, en contra de la privacidad personal, y, en suma de la información de carácter personal, no debe olvidarse que "es necesario que las medidas que se adopten respeten en todo caso los principios que configuran el contenido esencial del derecho a la protección de datos"[60].

[57] Bajo, "Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el *compliance*", 281.

[58] La Guía Legislativa de la OEA, por ejemplo, menciona que "los controladores de datos tienen el deber claro de tomar las medidas prácticas y técnicas que sean necesarias para proteger los datos personales que obren en su poder o bajo su custodia (o de los cuales sean responsables) y cerciorarse de que tales datos personales no sean objeto de acceso, pérdida, destrucción, uso, modificación o divulgación excepto con el conocimiento o consentimiento de la persona o de otra autoridad legítima. La obligación específica consiste en proporcionar salvaguardias razonables y adecuadas. Se basa en la consecución y el mantenimiento de un nivel apropiado de atención en el contexto de la situación general. Por lo tanto, hay que tener en cuenta consideraciones de proporcionalidad y necesidad".

[59] Ramon Oró, *La protección de datos*, (Barcelona: Oberta UOC, 2015), 67-68.

[60] Pablo Lucas Murillo de la Cueva y José Luis Piñar Mañas, El *derecho a la autodeterminación informativa* (Madrid-México: Fontamara S.A, 2011), 157.

### 2.4 Evaluación de impacto en el tratamiento de datos y consulta previa

Las evaluaciones de impacto obligan al responsable de tratamiento a realizar enfoques de riesgo "cuando las operaciones de tratamiento puedan poner en riesgo, de una manera significativa, los derechos y libertades de las personas cuyos datos van a ser objeto de tratamiento"[61]. Por una parte, a partir del art. 54 del PLODP 2019, la LOPD ha precisado que el responsable realizará una evaluación de impacto "cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular", la cual deberá efectuarse "previo al inicio del tratamiento de datos personales" –art. 42–[62]. Y por otra que, deberá "realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales" –art. 47.6–[63]. De esta manera, entendemos que:

> Las evaluaciones de impacto relativas a la protección de datos están estrechamente vinculadas a la protección de datos desde el diseño, ya que estas constituyen un verdadero proceso de reflexión que se aborda antes de iniciar las operaciones de tratamiento, es decir, la evaluación de impacto se hace en el momento en que se diseña una nueva aplicación, sistema de información, servicio, etc., en el que se esté planteando el uso de datos personales[64].

Nos parece que la LOPD sigue la línea del RGPD, puesto que éste señala que, cuando un tratamiento –realizado, particularmente, con nuevas tecnologías– pueda entrañar un alto riesgo para los derechos y libertades de las personas, "el

[61] Ramón Miralles López, "Evaluación de impacto relativa a la protección de datos y consulta previa (Arts. 35 y 36)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 471.

[62] En este caso, el RGPD determina que "el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento" –Considerando 90–.

[63] Con referencia a este aspecto, la Guía Legislativa de la OEA señala que "en los programas y procedimientos se deben tener en cuenta la índole de los datos personales en cuestión, el tamaño y la complejidad de la organización que recopila, almacena y procesa los datos, y el riesgo de violaciones. La protección de la privacidad depende de una evaluación creíble de los riesgos que el uso de datos personales podría plantear para las personas y la mitigación responsable de esos riesgos".

[64] Miralles López, "Evaluación de impacto relativa a la protección de datos y consulta previa (Arts. 35 y 36)", 471.

responsable del tratamiento realizará antes del tratamiento una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales" –art. 35.1–[65]. En el mismo sentido, en Ecuador, la normativa de protección de datos adoptaría el modelo de regulación de los EPEI, por cuanto este instrumento precisa que, cuando al llevar a cabo un tratamiento de datos se estime la probabilidad de un alto riesgo para los derechos de los titulares; la evaluación de impacto a la protección de datos es una obligación del responsable. Por tanto, "realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales" –art. 41.1–.

En todo caso, a diferencia del RGPD, la LOPD no determina que, al momento de realizar la evaluación de impacto, el responsable obtenga asesoría del delegado de protección de datos. Se trata de una previsión necesaria, por cuanto este asesoramiento constituye "una intervención activa en el diseño y ejecución de la evaluación, ya sea con funciones de coordinación o de interlocución principal con los evaluadores, o bien de colaboración con el evaluador, quedando como persona de contacto relevante dentro de la organización"[66].

> Es el DPD un instrumento que el Reglamento proporciona a los responsables y encargados del tratamiento para que éstos puedan cumplir el principio de responsabilidad proactiva (también podríamos mencionar a estos efectos los códigos de conducta o los mecanismos de certificación). Son dos a nuestro entender las características esenciales que el Reglamento atribuye al DPD: su cualificación, esto es, el conocimiento especializado del derecho y de la práctica de la protección de datos, y la independencia para el ejercicio de sus funciones[67].

Conviene precisar que en un inicio el PLODP 2019 no señala los supuestos en los que se requería realizar una evaluación de impacto[68]; y el contenido mínimo que

[65] Si bien las evaluaciones de impacto deben realizarse antes del tratamiento, "por supuesto no hay obstáculo en plantear una EIPD a tratamientos que ya estén implantados, ya que por definición la evaluación se concibe como un proceso repetible; en efecto, las evaluaciones realizadas deberán ser objeto de revisión, sea periódica o extraordinaria, para ir adaptando los tratamientos que en su día fueron evaluados, a las nuevas circunstancias y cambios que puedan afectarles". Miralles López, "Evaluación de impacto relativa a la protección de datos y consulta previa (Arts. 35 y 36)", 471-472.

[66] Miralles López, "Evaluación de impacto relativa a la protección de datos y consulta previa (Arts. 35 y 36)", 483.

[67] Aperribai Ulacia e Intxaurtieta Madariaga, "Consideraciones de la Agencia Vasca de Protección de Datos", 102.

[68] Según el RGPD, la evaluación se requerirá "en caso de: a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la

debía incluir la evaluación[69]. En efecto, esta omisión del legislador no podía pasar inadvertida, por cuanto los EPEI subrayan que las legislaciones deberán señalar "los tratamientos que requieran de una evaluación de impacto a la protección de datos personales; el contenido de éstas, los supuestos en que resulte procedente presentar el resultado ante la autoridad de control, así como los requerimientos de dicha presentación, entre otras cuestiones" –art. 41.2–. En todo caso, siguiendo las regulaciones del RGPD, únicamente, la LOPD ha concretado tres supuestos, por los cuales la evaluación de impacto es obligatoria. Por ejemplo, cuando se trate de: "evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales" –art. 42. a)–; "tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales" –art. 42. b)–; y, "observación sistemática a gran escala de una zona de acceso público" –art. 42. c)–.

elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o c) observación sistemática a gran escala de una zona de acceso público" –art. 35.3–.En este punto, resaltamos que "el art. 35.3 utiliza la expresión «en particular», de lo que se deduce que no estamos antes una lista exhaustiva o cerrada, podrán existir otros tipos de tratamientos que no estén incluidos en esos tres casos descritos que, sin encajar en ninguno de esos supuestos, también podrían presentar riesgos igualmente elevados". Miralles López, "Evaluación de impacto relativa a la protección de datos y consulta previa (Arts. 35 y 36)", 476.

[69] Así pues, el RGPD determina que la evaluación "deberá incluir como mínimo: a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas. –art. 35.7–. Sobre este respecto, advertimos que "el resultado final de realizar una evaluación de impacto deberá quedar documentado, debiendo recoger las características del tratamiento evaluado y las decisiones tomadas para mitigar los riesgos en base a la identificación, análisis y valoración de estos (gestión de los riesgos), incluyendo también cuestiones como el interés legítimo (en el caso de concurrir), y la necesidad y proporcionalidad de las operaciones de tratamiento" Miralles López, "Evaluación de impacto relativa a la protección de datos y consulta previa (Arts. 35 y 36)", 478.

Por último, hace falta que la LOPD establezca un deber de consulta a las partes afectadas en dichas evaluaciones. Como determina el RGPD, "cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento" –art. 35.9–. Así, "esa consulta a las futuras personas afectadas servirá para que, en su caso, sea tenida en cuenta tanto a la hora de valorar los potenciales riesgos, como cuando se seleccionen las medidas a adoptar para mitigarlos"[70].

Ahora bien, en relación a la consulta previa, el responsable del tratamiento debe consultar a la autoridad de control, luego de la evaluación de impacto, de que el tratamiento de la información entrañaría un alto riesgo, "debido a que el responsable del tratamiento no puede adoptar medidas para mitigar el riesgo, es decir, se da la circunstancia de que durante el proceso de evaluación el responsable del tratamiento no ha encontrado medidas suficientemente efectivas como para mantener controlados los riesgos en un nivel aceptable"[71]. Respecto a esta obligación, la LOPD no prevé que el responsable del tratamiento consulte a la autoridad de control, y que, además, ésta lo asesore por escrito, conforme el procedimiento contemplado en el RGPD[72]. Así, subrayamos que, "siempre que el responsable del fichero considere que el tratamiento de datos previsto pudiera entrañar riesgos para los titulares de los datos, deberá plantear una consulta previa ante la autoridad de control correspondiente"[73]. Por tanto, esta omisión legislativa en la normativa de protección de datos significa el mejor escenario para introducir

[70] Miralles López, "Evaluación de impacto relativa a la protección de datos y consulta previa (Arts. 35 y 36)", 483.
[71] Ibíd., 490.
[72] El RGPD determina que, cuando el responsable consulte a la autoridad de control, le facilitará la información siguiente: "a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial; b) los fines y medios del tratamiento previsto; c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados; d) en su caso, los datos de contacto del delegado de protección de datos; e) la evaluación de impacto relativa a la protección de datos, y f) cualquier otra información que solicite la autoridad de control" –art. 36.3–.
[73] José María Pérez Gómez, "Especialidades en el sector sanitario", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 205.

esta obligación. Bien, a través de su reglamentación o, mediante su adecuación en la norma técnica, que emita la Autoridad de Protección de Datos. Este cambio en la LOPD podría seguir la regulación contenida en el RGPD, que sobre la consulta previa señala que, el responsable "consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo" –art. 36.1–[74].

### 2.5 El delegado de protección de datos

Podemos advertir que, otra medida proactiva que deben asumir los responsables y encargados del tratamiento, es la designación de un delegado de protección de datos o *Data Protection Officer* que informe, asesore y supervise "aquellos tratamientos que requieran una observación habitual y sistemática de interesados a gran escala y para los tratamientos a gran escala de categorías especiales de datos o de datos relativos a condenas o a infracciones penales"[75]. Así, "este DPD deberá contar con la confianza, profesional y ética, de su Responsable/ encargado, siendo leal a este, todo ello manteniendo su independencia. No recibir presiones o no sucumbir a ellas distinguirá a un Responsable concienciado y a un DPD que actúa con todas las garantías"[76].

En primer término, el RGPD dispone que el responsable y encargado designarán un delegado, cuando: "el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial" –art.

[74] El RGPD añade que, "la autoridad de control debe responder a la solicitud de consulta dentro de un plazo determinado. Sin embargo, la ausencia de respuesta de la autoridad de control dentro de dicho plazo no debe obstar a cualquier intervención de dicha autoridad basada en las funciones y poderes que le atribuye el presente Reglamento, incluido el poder de prohibir operaciones de tratamiento. Como parte de dicho proceso de consulta, se puede presentar a la autoridad de control el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas" –Considerando 94–.

[75] Troncoso, "Autoridades de Control Independientes", 466.

[76] Carme Sánchez Ors, "El Delegado de Protección de Datos. Guardián de la Privacidad (Arts. 37, 38 y 39)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 494.

37.1 a)–; “las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o” –art. 37.1 b)–; “las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales” –art. 37.1 c)–. Asimismo, la LOPDGDD señala que, los responsables y encargados “deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679” –art. 34.1–. Esta Ley, registra a las entidades que les corresponde hacerlo[77].

Frente a este marco, el PLODP 2019 fue la única propuesta que hizo referencia al delegado de protección de datos. Naturalmente, a la luz de dicha propuesta, la LOPD, en primer término, determina que, como una obligación del responsable del tratamiento se deberá “designar al Delegado de Protección de Datos Personales, en los casos que corresponda” –art. 47.13–. En este orden, los supuestos en los cuales se designará un delegado son cuando: “el tratamiento se lleve a cabo por quienes conforman el sector público de acuerdo con lo establecido en el artículo 225 de la Constitución de la República” –art. 48.1–[78]; “las actividades del responsable o encargado del tratamiento requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades del tratamiento” –art. 48.2–; “se refiera al tratamiento de gran volumen de categorías especiales de datos” –art. 48.3–; y “el tratamiento no se refiera a datos relacionados con la seguridad nacional y defensa del Estado que adolezcan de reserva ni fuesen secretos, de conformidad con lo establecido en la normativa especializada en la materia” –art. 48.4–.

[77] Véase el art. 34.1 de la LOPDGDD, en el cual se señalan las entidades que deben designar un Delegado de Protección de Datos.

[78] El art. 225 de la Constitución de Ecuador establece que, “el sector público comprende: 1. Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social. 2. Las entidades que integran el régimen autónomo descentralizado. 3. Los organismos y entidades creados por la Constitución o la Ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado. 4. Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos”.

En este orden, la LOPD sigue el esquema de regulación de la normativa europea que queda anotada. Y, en todo caso, establece las prescripciones señaladas en los EPEI, ya que, el delegado –oficial de protección de datos, según este instrumento– será designado por el responsable, cuando: "sea una autoridad pública" –art. 39.1.a)–; "lleve a cabo tratamientos de datos personales que tengan por objeto una observación habitual y sistemática de la conducta del titular" –art. 39.1.b)–; y "realice tratamientos de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares", como el caso de los datos sensibles –art. 39.1.c)–.

No obstante, a diferencia del RGPD y de la LOPDGDD, la normativa de protección de datos de Ecuador omite señalar que los responsables y encargados del tratamiento, sean quienes deban designar al delegado de protección de datos. Si bien en las obligaciones del responsable se advierte que esta es su obligación –art. 47.13–; en las disposiciones relativas al delegado de protección de datos, únicamente, se determina que "se designará un delegado de protección de datos" –art. 48–. En este marco, advertimos que:

> En función de quien cumpla los criterios sobre designación obligatoria este será quien ineludiblemente deberá disponer de la figura, en algunos casos será únicamente uno de ellos, mientras que en otros ambos estarán obligados a nombrar un DPD siendo necesaria su colaboración. No obstante, en situaciones en que el Responsable deba disponer de un DPD, dado su papel central para el cumplimiento, especialmente a la luz de las nuevas obligaciones destinadas a conseguir una protección de datos más eficaz, puede ser una buena práctica que su Encargado también lo nombre. En cualquier caso, la designación de un DPD confiere una protección adicional a los tratamientos que se vayan a realizar y promociona la protección efectiva de los datos como una ventaja competitiva[79].

Además, otra diferencia está relacionada con las entidades u organismos públicos que deben designar al delegado. Así, la LOPD también extiende esta obligación a la función judicial. En este punto, aclaramos que el art. 37.1. a) del RGPD plantea este supuesto como una excepción. Ahora bien, por una parte, llamaba la atención que el art. 58 *in fine* del PLODP 2019 disponga que la autoridad de control podría "definir nuevas condiciones para la necesidad de contar con un Delegado de Protección de Datos Personales, así como emitir directrices para su designación";

[79] Sánchez Ors, "El Delegado de Protección de Datos. Guardián de la Privacidad (Arts. 37, 38 y 39)", 520.

y, por otra, también que dicha autoridad, según el art. 60 *in fine* de dicha propuesta, pueda definir "otras funciones, atribuciones y responsabilidades para el delegado de protección de datos personales". Sobre este respecto, apuntamos que el RGPD señala que el responsable y el encargado del tratamiento "garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones" –art. 38.3–. Así también, en relación a la posición del delegado de protección de datos, la LOPDGDD (art. 36.1) añade que el delegado "actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos" –art. 36.1–; y en todo caso, se reconoce que se garantizará "la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses " –art. 36.2–.

En todo caso, si bien la LOPD ha ratificado que la autoridad de control "podrá definir nuevas condiciones en las que deba designarse un delegado de protección de datos personales y emitirá, a dicho efecto, las directrices suficientes para su designación" –art. 48 *in fine*–; en lo que corresponde a la definición de otras funciones, la normativa de protección de datos plantea que "siempre que no exista conflicto con las responsabilidades establecidas en la presente ley, su reglamento, directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales, el delegado de protección de datos personales podrá desempeñar otras funciones dispuestas por el responsable o el encargado del tratamiento de datos personales" –art. 50 *in fine*–. De esta manera, subrayamos que:

> Los DPD, tanto de responsables como de encargados, deben ser independientes y capaces de actuar sin restricciones, dirección o instrucciones sobre cómo realizar sus tareas o el resultado de estas. Esta independencia la deben garantizar sus empleadores y los propios DPD que no deben dejarse influir o presionar de manera que se comprometan sus funciones (…) La independencia del DPD no se debe interpretar para convertirlo ni en una «miniautoridad de protección de datos». Su independencia debe garantizarse con una persona íntegra y leal. De la misma manera, en la organización debe ser vista como alguien con prestigio profesional y con cierto poder suficiente para desarrollar sus funciones. Esto requiere por un lado un puesto patrocinado por los órganos de decisión de la organización, una línea de reporte directo a la dirección de la organización y recursos apropiados, y por

> otro debe primar el vínculo entre el DPD y los miembros de su organización en los valores éticos, morales y motivacionales que se comparten[80].

Nos parece que, el PLODP 2019 al permitir que la autoridad de control establezca condiciones, emita directrices, defina otras funciones, atribuciones y responsabilidades para el delegado de protección de datos; esto hubiese afectado al desempeño de sus funciones y dejaría de garantizar su independencia. Como hemos indicado, debe garantizarse que el delegado no reciba instrucciones. En cualquier caso, una cuestión distinta es que el delegado coopere con la autoridad de control. Así, según dispone el art. 39.1. d) del RGPD, una de las funciones del delegado de protección de datos es "cooperar con la autoridad de control".

> Algunas voces ven en esta cooperación que la autoridad de control tiene un «topo» en su organización, pero debe ser visto más como un reconocimiento general a los profesionales y su importancia. Desde una perspectiva oficial, puede parecer que la autoridad de control tiene un «funcionario» designado dentro de la organización con el cual pueden contactar y tratar inmediatamente, tanto en un sentido rutinario como también cuando surgen problemas. Esta cooperación ayudará a crear una línea de comunicación más rápida y eficiente que sólo aumentará con el tiempo como línea dedicada de comunicación y contacto entre el DPD de la organización y la autoridad de control[81].

Con relación a este aspecto, identificamos que este constituye un supuesto que sí está prescrito en el art. 49.4 de la LOPD, por el cual, se determina que una de las funciones del delegado es "cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos". En otro orden de cosas, la LOPD no establece que el delegado sea elegido sobre la base de sus cualidades profesionales. Así, como determina el RGPD, éste "será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos" –art. 37.5–. Así, frente a la designación del delegado, es fundamental regular que el responsable o el encargado lo designen, considerando "el nivel de experiencia, conocimientos y destrezas necesarias o asumibles por la organización. Para ello deberán tener en

[80] Ibíd., 501.
[81] Ibíd., 513.

cuenta las operaciones de tratamiento que se lleven a cabo y la protección exigida para los datos personales tratados"[82].

Hasta aquí, nos parece que el PLODP 2016 presentaba una serie de limitaciones, frente al ámbito de regulación que plantea la comunidad internacional, en relación a las obligaciones de los responsables del tratamiento. No obstante, el PLODP 2019 planteó un esquema de regulación similar al RGPD, la LOPDGDD y los lineamientos establecidos en los EPEI. Sin duda, sobre la base de dicha propuesta, la normativa de protección de datos aprobada en mayo de 2021 favorecerá a la implementación de medidas proactivas, técnicas y organizativas, las cuales deberán ser adoptadas por los responsables para garantizar el cumplimiento de la legislación de protección de datos. Como destacamos:

> Estas medidas, junto con otras como la realización de informes de impacto en la protección de datos personales, la implementación de mecanismos de verificación y auditoría de carácter jurídico o la designación de un delegado de protección de datos (…) tratan de introducir la protección de datos dentro de la responsabilidad empresarial, convirtiendo a las empresas en un elemento estratégico en el sistema de garantías del derecho a la protección de datos personales, que haga compatible un uso intensivo de las tecnologías y el tratamiento de datos personales necesarios para el funcionamiento global de la economía con el respeto a la privacidad de los usuarios y de los empleados[83].

Si bien, hemos expuesto algunas precisiones que deben reformularse en la LOPD, consideramos que el momento oportuno para introducir dichas reformas es en el debate legislativo que considere la reglamentación de dicha norma.

### 2.6 Crítica a otras obligaciones enmarcadas en el proyecto de Ley de 2016

El art. 8 del PLODP 2016 determinaba algunas obligaciones del responsable del tratamiento, que tenían relación con la información y acceso a los datos personales. Así, por ejemplo, encontramos:

1. Requerir y obtener el consentimiento del titular de los datos personales, previo a su obtención y tratamiento.

[82] Ibíd., 507.
[83] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 53.

2. Informar al titular de los datos, en forma expresa y clara, previamente a recabar información referida a su persona, acerca de:
   a) La existencia del archivo, registro, base o banco de datos, electrónico o de cualquier tipo de que se trate y la identidad y domicilio de su responsable.
   b) La finalidad para la que serán tratados y quienes pueden ser sus destinatarios o categorías de destinatarios.
   c) El carácter obligatorio o facultativo de la respuesta a las preguntas que le sean formuladas.
   d) Las consecuencias que se deriven por proporcionar los datos, por la negativa a hacerlo o por la inexactitud de los mismos.
   e) La facultad y modo de ejercer los derechos de acceso rectificación, actualización y supresión de los datos que le confiere la presente Ley.
3. Proceder en forma inmediata a la rectificación, actualización o supresión, de los datos personales cuando fueran total o parcialmente inexactos, incompletos o desactualizados.
4. Inscribir sus archivos, registros, bases o bancos de datos en el Registro Nacional de Bases de Datos creado por el organismo de control[84].

Conviene aclarar que el RGPD regula, tanto la información que deberá facilitarse, cuando los datos personales se hayan obtenido del interesado como la información que deberá facilitarse, cuando los datos no se hayan obtenido del interesado. Así, el RGPD dispone que "cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan" –art. 13.1–, le facilitará la siguiente información:

> a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
> b) los datos de contacto del delegado de protección de datos, en su caso;
> c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
> d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
> e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
> f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo

[84] Si bien en el contexto europeo existía la obligación de inscribir y notificar el tratamiento de datos a las autoridades de control, en la actualidad, el RGPD refiere que esta obligación no contribuyó a mejorar los niveles de protección de datos. En este contexto, el Reglamento precisa que "estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial" –Considerando 89–.

49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado[85].

Además, el art. 14.1 del RGPD prescribe que, en los casos, en los cuales los datos personales no se hubieran obtenido del interesado; el responsable está obligado a facilitar la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;
d) las categorías de datos personales de que se trate;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado[86].

[85] En este punto, el RGPD agrega que "además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo; b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada; d) el derecho a presentar una reclamación ante una autoridad de control; e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos; f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado" –art. 13.2–.

[86] Con relación a este aspecto, el RGPD apunta que "además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado: a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo; b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero; c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada; e) el derecho a presentar una reclamación ante una autoridad de control; f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público; g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información

Sobre estos supuestos de información y acceso a los datos personales, de conformidad al PLODP 2019, la LOPD ha concretado que, en los casos en que los datos personales sean obtenidos, directamente, del titular, "la información deberá ser comunicada de forma previa a este, es decir, en el momento mismo de la recogida del dato personal"; y excepcionalmente, cuando los datos personales fueren obtenidos de una fuente accesible al público o no sean obtenidos del titular, éste "deberá ser informado dentro de los siguientes treinta (30) días o al momento de la primera comunicación con el titular, cualquiera de las dos circunstancias que ocurra primero" –art. 12 *in fine*–.

Como hemos indicado en otro momento, no se puede ejercer el derecho a la protección de datos, "entendido como el derecho al control sobre la propia información personal, si se desconoce cuáles son las finalidades que justifican el tratamiento de la información personal, quién es el responsable ante el cual se pueden ejercitar los derechos y cuáles son los posibles cesionarios"[87]. Por esta razón, especial importancia tiene la obligación de informar, previamente, a los titulares de los datos personales, sobre la existencia de un archivo, registro, base o banco de datos, con inclusión de la identidad y domicilio del responsable del tratamiento, a fin de que se puedan ejercitar los derechos de acceso, rectificación, actualización y supresión de los datos.

La obligación de informar sobre la finalidad para los que serán tratados y quiénes pueden ser sus destinatarios, categorías de destinatarios o cesionarios; reviste otro de los aspectos más importantes dentro del tratamiento, ya que, como aclara la CCE, en el respeto del derecho a la protección de datos, "las personas puedan obtener el conocimiento de los datos a ellos referidos, y advertirse sobre su finalidad, sea que dicha información conste en el registro o banco de datos público

significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado" –art. 14.2–.

[87] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 453. Hay que considerar que, según la Guía legislativa de la OEA, "a fin de que las personas cuenten con fundamentos para decidir a quiénes proporcionarán sus datos personales y por qué razón, posiblemente se necesite más información que los meros fines de la recopilación y el manejo de esos datos".

o privado”[88]. Por ello, “si se van a utilizar los datos para una finalidad distinta, hay que volver a informar”[89]. Para este fin, es esencial la obligación de requerir y obtener el consentimiento del titular de los datos personales. Además, hay que advertir que “el consentimiento del interesado no convalida un tratamiento de datos personales excesivos que vaya más allá de la finalidad”[90].

En todo caso, es significativo estimar que “la ausencia del consentimiento del interesado –en un derecho que también se denomina de autodeterminación informativa por la importancia que atribuye al consentimiento del interesado– obliga a reforzar el resto de principios de protección de datos”[91]. De este modo, las instituciones públicas y privadas –en suma, los responsables y encargados del tratamiento– como garantes de la Constitución tienen la obligación de asegurar el respeto del derecho a la protección de datos. Por cuanto, como advierte la CCE, frente al tratamiento de la información personal, el titular o interesado “tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de su información personal y el tiempo de vigencia del archivo o banco de datos”[92].

### 3. Obligaciones del encargado

[88] Véase la Resolución de la Corte Constitucional 182, Sentencia Nro. 182-15-SEP-CC –Caso Nro. 1493-10-EP– publicada en el Registro Oficial Suplemento Nro. 607 de 14 de octubre de 2015. Así también la Guía legislativa de la OEA considera que: “no deben mantenerse ni utilizarse datos personales con fines que no sean compatibles con aquellos para los cuales se hayan recopilado, excepto con el conocimiento o consentimiento del titular de los datos o por mandato de la Ley. El concepto de “incompatibilidad” da cierto grado de flexibilidad, ya que permite hacer referencia al objetivo o propósito general en relación con el cual la persona haya dado inicialmente su consentimiento para que se recopilaran datos. En ese sentido, la medida apropiada suele consistir en respetar el contexto en el cual la persona haya proporcionado sus datos personales y las expectativas razonables de la persona en esa situación particular”.

[89] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 453**.**

[90] Ibíd., 466.

[91] Ibíd., 454.

[92] Tal como destaca la Guía legislativa de la OEA: “se deben especificar los fines para los cuales se recopilan los datos personales en el momento en que se recopilen. Como regla general, los datos personales solamente deben ser recopilados con el consentimiento de la persona a que se refieran”. Esto implica considerar el principio de transparencia dentro del tratamiento de la información personal, por ello este instrumento agrega que: *“*los fines para los cuales se recopilan datos personales deben especificarse claramente en el momento en el cual se recopilen”.

Recordemos que, conjuntamente, con los responsables del tratamiento, el encargado tiene la obligación de garantizar y supervisar que el tratamiento de datos respete el derecho a la protección de datos de los titulares. Así, atendiendo el principio de responsabilidad demostrada, se pretende que "el responsable o encargado del tratamiento actúe con diligencia debida mediante este principio de responsabilidad proactiva, gestionando los riesgos mediante un sistema de control interno sólido"[93]. De tal modo que, las medidas y técnicas que utilice el encargado, por vía manual o telemática, estén orientadas a impedir intromisiones ilegítimas en los derechos y libertades de los titulares. En todo caso, es primordial que el encargado ofrezca conocimientos especializados, fiabilidad y recursos que garanticen que el tratamiento cumpla con la legislación de protección de datos[94].

Por ejemplo, el RGPD establece que se debe elegir "un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado" –art. 28.1–. En este sentido, los EPEI coinciden en que éste deberá "implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables" –art. 34.3.c)–. De esta manera, respecto a las obligaciones del encargado, el PLODP 2016 se limitó, únicamente, a señalar que le correspondían a éste las mismas obligaciones exigidas al responsable, "tanto respecto de la confidencialidad y reserva que debe mantener sobre la información obtenida, como del respeto y cumplimiento de los principios generales de la protección de datos" –art. 9–. Si bien era una disposición bastante general, nos parece que –conforme a las obligaciones del responsable que fueron analizadas en el apartado anterior–; esta propuesta no garantizaba que el

[93] Bajo, "Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el *compliance*", 282.

[94] El RGPD señala que, "para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento" –Considerando 81–.

encargado del tratamiento cumpliera con la legislación de protección de datos, ni tampoco ofreciera las suficientes garantías para los derechos de los titulares. Desde esta perspectiva, entendemos que una correcta regulación de las exigencias que les corresponden a los encargados persigue involucrar a éstos "en la obligación de control y diligencia debida, quien, gracias a su posición en la relación de tratamiento de datos, puede detectar de una manera más rápida que el responsable, la producción de una fuga de datos"[95].

En este marco, si bien el PLODP 2019 propuso un conjunto de obligaciones, a la luz de la normativa del RGPD; finalmente, el legislador ha dispuesto en la LOPD que tan solo le corresponde al encargado del tratamiento "las mismas obligaciones que el responsable de tratamiento de datos personales, en lo que sea aplicable, de acuerdo a la presente ley y su reglamento" –art. 47 *in fine*–. Sin existir precisiones, dentro del Informe para segundo debate del Proyecto de Ley Orgánica de Protección de Datos Personales, por las cuales el legislador decidió prescindir de las obligaciones que corresponden al encargado del tratamiento[96]; atendiendo la normativa internacional, consideramos oportuno abordar la naturaleza de éstas a la luz de la última propuesta normativa.

El PLODP 2019 determinaba que, como parte de las obligaciones del responsable, éste elegirá y designará un encargado que "ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme lo establecido en la presente Ley, reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales" –art. 71.12–. Precisamente, conviene aclarar que esta obligación sí forma parte de la LOPD, toda vez que, como parte de las obligaciones del responsable se determina que éste deberá asegurar que el encargado "ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de

[95] Francisco Pérez Bes, "La obligación de notificar una violación de seguridad de datos personales", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 462.
[96] El Informe para segundo debate del Proyecto de Ley Orgánica de Protección de Datos Personales puede consultarse en: https://leyes.asambleanacional.gob.ec/.

Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional" –art. 47.11–.

Ahora bien, dentro de las obligaciones que corresponden al encargado, el PLODP 2019 agregaba que éste estaría obligado a "tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia" –art. 72.1–. Por una parte, llamaba la atención que las condiciones que debe reunir el encargado formen parte de las obligaciones que regulan las actividades de los responsables del tratamiento. Por otra, tomando en cuenta que el tratamiento por el encargado se regirá por un contrato, el RGPD determina que el encargado "tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional" –art. 28.3 a)–[97]. Nos parece que la disposición sobre acatar directrices, lineamientos y regulaciones de la autoridad de control, por parte del encargado del tratamiento, no constituía una obligación que debía ser impuesta por la autoridad. Más bien, las obligaciones del encargado tenían que ajustarse a las instrucciones del responsable, siguiendo el contrato o acto jurídico que vincule al encargado con el responsable del tratamiento[98].

[97] El RGPD señala que "el tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado" –Considerando 81–. Además, lo ratifica los EPEI al precisar que el encargado deberá realizar "el tratamiento de los datos personales conforme a las instrucciones del responsable" –art. 34.3. a)–.

[98] En todo caso, "respecto de las instrucciones, la AEPD ha dictado las siguientes directrices: «Se debe documentar de forma precisa las instrucciones respecto del encargo realizado. Es necesario identificar de forma clara y concreta cuáles son los tratamientos de datos a realizar por el encargado del tratamiento, atendiendo al tipo de servicio prestado y a la forma de prestarlo. Es especialmente necesario determinar de forma clara las comunicaciones a terceros que el responsable encomienda al encargado o que se derivan del servicio prestado»". Cfr. Cecilia Álvarez Rigaudias, "El tratamiento y sus responsables", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 437.

Así pues, el RGPD establece que el tratamiento por el encargado "se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable" –art. 28.3–. Y, además, los EPEI precisan que "la prestación de servicios entre el responsable y encargado se formalizará mediante la suscripción de un contrato o cualquier otro instrumento jurídico" –art. 34.1–. En este caso, si bien, no se precisa la obligación de seguir las instrucciones del responsable; advertimos que ésta sí era una previsión contenida en el PLODP 2019, por cuanto se estipulaba que era una obligación del encargado "tratar datos personales de conformidad a lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales inclusive en lo que respecta a la transferencia o comunicación internacional" –art. 72.2–.

Como hemos destacado, del contrato o acto jurídico que vincula al encargado y al responsable del tratamiento, se determina en gran parte las obligaciones de aquél. El RGPD dispone que dicho contrato estipulará que el encargado está obligado a garantizar que "las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria" –art. 28.3. b)–. En este sentido, los EPEI coinciden en que el encargado debe "guardar confidencialidad respecto de los datos personales tratados" –art. 34.3. e)–. Siguiendo este esquema, el PLODP 2019 estableció que el encargado tiene la obligación de "garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales" –art. 72.4–; y que, también debía "suscribir contratos de confidencialidad y manejo adecuado de datos personales con el personal a cargo del tratamiento de datos" –art. 72.3–. En efecto:

> El ET debe adoptar las medidas técnicas y organizativas necesarias para proteger los datos personales contra el tratamiento no autorizado o ilegal y contra la pérdida accidental, destrucción o daño de los datos personales y que: (i) sean aptas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia constante de los sistemas y servicios de tratamiento (p. ej., aplicando, en su caso, técnicas de pseudonimización y/o cifrado); (ii) permitan restaurar la disponibilidad y el acceso a los datos personales en caso de incidencia física o técnica; e (iii) incluyan un proceso para evaluar regularmente su efectividad. Las

> obligaciones de confidencialidad bajo (i) incluirán que el ET se asegure de que los empleados que se ocupan del tratamiento de datos personales estén obligados al secreto de datos[99].

Ahora bien, el RGPD dispone que el encargado "tomará todas las medidas necesarias de conformidad con el artículo 32" –art. 28.3. c)–. Esto es, en lo relativo a las garantías de seguridad de los datos[100]. En este marco, asimismo, los EPEI consideran que los encargados deben "informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones" –art. 34.3. d)–. En esta línea, el PLODP 2019 determinó que el encargado debería "implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar vulneraciones" –art. 72.5–. Por tanto, correspondía una obligación "de notificación que recae sobre el encargado del tratamiento, quien deberá notificar sin dilación indebida al responsable del tratamiento las violaciones de seguridad de los datos personales de las que tenga conocimiento"[101].

Por otra parte, el RGPD apunta que el encargado "asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados" –art. 28.3. e)–[102]. Al respecto, los EPEI, bajo una prescripción bastante general, señalan que debe "colaborar con el responsable en todo lo relativo al cumplimiento de la legislación nacional" –art. 34.3. j)–. Adoptando ambos esquemas, el PLODP 2019 expuso que el encargado tendría que asistir al responsable "para que este cumpla con su obligación de atender solicitudes que

[99] Álvarez Rigaudias, "El tratamiento y sus responsables", 438.

[100] Recordemos que el RGPD prescribe que "al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales" –Considerando 83–.

[101] Pérez Bes, "La obligación de notificar una violación de seguridad de datos personales", 462.

[102] Por ejemplo, el RGPD determina que el encargado del tratamiento "debe asistir al responsable cuando sea necesario y a petición suya, a fin de asegurar que se cumplen las obligaciones que se derivan de la realización de las evaluaciones de impacto relativas a la protección de datos y de la consulta previa a la autoridad de control" –Considerando 95–.

tengan por objeto el ejercicio de los derechos del titular frente al tratamiento de sus datos personales" –art. 72.6–; y, así también para "garantizar el cumplimiento de las obligaciones previstas en la presente Ley" –art. 72.7–. En este aspecto, el encargado tendría que colaborar con el responsable a responder "en tiempo y forma a las solicitudes de ejercicio de los derechos del interesado (en particular, si recibe alguna de estas solicitudes, notificará tales solicitudes de forma inmediata al RT junto con la información de que disponga (en su caso) que pueda ser relevante para responder a la solicitud"[103].

Además, el RGPD determina que el encargado "a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales" –art. 28.3. g)–. Esta es una obligación que también está contenida en los EPEI, por la cual el encargado podrá "suprimir, devolver o comunicar a un nuevo encargado designado por el responsable los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones de éste" –art. 34.3. f)–[104]. Con referencia a este aspecto, el PLODP 2019 señaló la obligación de "transferir o comunicar los datos personales entregados al responsable del tratamiento y suprimirlos una vez que haya finalizado su encargo" –art. 72.8–. Así, mediante esta disposición se aseguró que el encargado debería "devolver o destruir los datos personales del RT (según decida el RT) una vez finalizada la prestación de los servicios de los que trae causa el encargo y eliminar de forma segura las copias existentes"[105].

Por último, el RGPD, en razón del contrato o acto jurídico, establece que el encargado deberá poner a disposición del responsable "toda la información necesaria para demostrar el cumplimiento de las obligaciones, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable" –art. 28.3. h)–

[103] Álvarez Rigaudias, "El tratamiento y sus responsables", 438.
[104] En este contexto, los EPEI agregan que, no corresponderá al encargado esta obligación, "excepto que una disposición legal exija la conservación de los datos personales, o bien, que el responsable autorice la comunicación de éstos a otro encargado" –art. 34.3. f)–.
[105] Álvarez Rigaudias, "El tratamiento y sus responsables", 439.

Sobre esta obligación, los EPEI precisan que deberá "permitir al responsable o autoridad de control inspecciones y verificaciones en sitio" –art. 34.3. h)–; y, además, "generar, actualizar y conservar la documentación que sea necesaria y que le permita acreditar sus obligaciones" –art. 34.3. i)–. En este contexto, el PLODP 2019 señalaba que debería "facilitar el acceso al responsable del tratamiento de datos personales de toda la información referente al cumplimiento de las obligaciones establecidas en la presente Ley" –art. 72.9–; y "permitir y contribuir a la realización de auditorías o inspecciones por parte del responsable del tratamiento o de un auditor autorizado por éste o por la Autoridad de Protección de Datos Personales" –art. 72.10–.

Pues bien, consideramos que estas obligaciones se concentran en el concepto de diligencia debida, por el cual, tanto el responsable como el encargado del tratamiento acreditan un sistema de control y contribución para la garantía del derecho a la protección de datos. Por tanto, es importante considerar que:

> La diligencia debida se compone de cuatro elementos: identificar, prevenir, mitigar y la rendición de cuentas, es decir: 1. Una evaluación del impacto real y potencial de las actividades sobre los datos (evaluación de riesgos). La integración de las conclusiones, y la actuación al respecto (los controles). 2. 3. 4. El seguimiento y monitoreo (evaluación del desempeño). La comunicación de la forma en que se hace frente a las consecuencias negativas (rendición de cuentas). Todo ello dentro de un proceso continuo. La diligencia debida proporciona una defensa contra la responsabilidad, permite una reducción de las sanciones o brinda un recurso de defensa cuando la empresa puede probar que había implementado los «procedimientos adecuados» para prevenir un impacto[106].

Hay que mencionar que, el PLODP 2019 concretaba que el encargado cumpliría "con el código de protección, mecanismos de certificación o sellos aprobados para demostrar la existencia de garantías suficientes para la protección de datos" –art. 72.11–[107]. Éstas tratan de unas obligaciones reconocidas en el RGPD, por cuanto se considera que "la adhesión del encargado del tratamiento a un código de conducta aprobado o a un mecanismo de certificación podrá utilizarse como

[106] Bajo, "Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el *compliance*", 282.

[107] Al respecto, advertimos que el RGPD señala que "a fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes" –Considerando 100–.

elemento para demostrar la existencia de las garantías suficientes" –art. 28.5–. Por tanto, en la implementación de estos instrumentos que permiten demostrar el cumplimiento de la legislación "como son los códigos de conducta o las normas corporativas vinculantes, es necesario que los mismos incluyan y detallen los mecanismos previstos para regular una comunicación continua con la autoridad de control, poniendo a su disposición toda la documentación de controles y verificaciones"[108].

A diferencia de la normativa internacional, el PLODP 2019 omitió considerar disposiciones relacionadas con la subcontratación de servicios por el encargado. En este caso, el RGPD precisa que "cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico (…) las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado" –art. 28.4–[109]. Asimismo, los EPEI apuntan que el encargado podrá "subcontratar servicios que impliquen el tratamiento de datos personales, siempre y cuando exista una autorización previa por escrito, específica o general del responsable, o bien, se estipule expresamente en el contrato o instrumento jurídico suscrito entre este último y el encargado" –art. 35.1–. Por tanto, "el subcontratado asumirá el carácter de encargado" –art. 35.2–.

Sin duda, tanto el responsable como el encargado del tratamiento, son determinantes a la hora de materializar el marco de protección de datos personales. En el caso del encargado es quien "actúa, de cara al ciudadano, en nombre del

[108] Blanco Antón, "Cooperación con la autoridad de control (Art. 31)", 452.

[109] El RGPD agrega que, "en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado" –art. 28.4–.

responsable y por cuenta de éste, como si fuera éste"[110]. Por ello, conforme a la normativa europea que queda expuesta, advertimos que:

> Hay que elegir un encargado que ofrezca garantías suficientes para implementar las medidas apropiadas -existe una responsabilidad *in eligendo*, a la que ya hacía mención la Directiva en relación con la seguridad-, que el encargado empleará únicamente a personal que se haya comprometido a respetar la confidencialidad o esté sujeto a una obligación legal de confidencialidad, que el encargado tiene la posibilidad de ayudar al responsable a garantizar el cumplimiento de sus obligaciones y que la relación entre el responsable y el encargado se documentará por escrito, debiendo constar las instrucciones del responsable y las obligaciones del encargado[111].

A partir del desarrollo tecnológico, es imprescindible que, tanto responsables como encargados del tratamiento, adopten las suficientes salvaguardias, técnicas y organizativas, que garanticen el derecho a la protección de datos. Siendo un derecho que corresponde a toda la sociedad, es imperativo contemplar medidas razonables y adecuadas, más aún, si se tiene en cuenta que existen datos sensibles que precisan de un nivel más alto de protección. Además, con relación a las obligaciones que quedan anotadas, advertimos la necesidad de que los responsables y encargados, se rodeen de profesionales con conocimientos especializados en materia de protección de datos[112].

Finalmente, recalcamos que a diferencia de la propuesta legal de 2019, el PLODP 2016 presentó serias limitaciones, frente a las obligaciones que corresponden, tanto a los responsables como encargados. Un ejemplo de aquello es que, reiteradamente, el PLODP 2016 confundió al encargado del tratamiento al atribuirle el carácter de "responsable de las bases de datos o banco de datos, ficheros y archivos". Por ello, reiteramos que el encargado "se limita a llevar a cabo el

---

[110] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 343**.**

[111] Troncoso, "Hacia un nuevo marco jurídico europeo de la protección de datos personales", 92.

[112] En este punto, el RGPD determina que "al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial (…) El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente" –Considerando 97–.

tratamiento de datos personales para el desarrollo de la gestión encomendada, cumpliendo en todo momento las instrucciones del responsable"[113]. En este orden de ideas, el legislador hizo una incorrecta interpretación al apreciar que quien actuaba bajo instrucciones era el encargado del tratamiento o responsable del tratamiento de la información; y no, el responsable o "encargado" de las bases de datos[114]. En este marco, es importante aclarar e individualizar las obligaciones que corresponden a todos aquellos que intervienen en el tratamiento de la información personal. La definición de las obligaciones, decisiones, procedimientos y mecanismos de protección, plantea una serie de cuestiones que requieren especial atención, toda vez, que el *habeas data* –como un derecho fundamental en sí mismo, para la protección de los datos– se caracteriza, pasivamente, "por los límites opuestos a quienes desde los poderes públicos o desde la sociedad utilizan información de carácter personal"[115].

Bajo estas consideraciones, apreciamos que el PLODP 2016 precisaba una serie de carencias en relación a los deberes y obligaciones que corresponden a los responsables y encargados del tratamiento. No obstante, a pesar de las observaciones anotadas al PLODP 2019 y a la misma LOPD, en cuanto a las obligaciones del encargado, la normativa de protección de datos aprobada en el 2021 significa un acertado avance en el desarrollo legislativo, sobre este derecho fundamental. En consecuencia, si consideramos que uno de los objetivos de la protección de datos es generar confianza y equilibrio. Sobre todo, en una sociedad digital en donde la información personal abunda y representa un valor económico.

[113] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 342.

[114] Con referencia a este supuesto, la Guía legislativa de la OEA advierte que el derecho fundamental a la protección de datos, "no es absoluto, sino contingente y contextual, y requiere un equilibrio difícil de intereses y principios. El ejercicio del derecho plantea necesariamente cuestiones fundamentales en lo que se refiere no solo a la privacidad, el honor y la dignidad, sino también al derecho de acceso a la verdad, la libertad de información y de expresión, y la proporcionalidad. También plantea cuestiones difíciles con respecto a quién toma tales decisiones y por medio de qué proceso y si la obligación se aplica solamente al recopilador original (o primario) de los datos en cuestión (controlador de datos) o también a intermediarios subsiguientes".

[115] Lucas Murillo de la Cueva y Piñar Mañas, El *derecho a la autodeterminación informativa*, 18.

# CAPÍTULO VII: LA PROTECCIÓN DE DATOS PERSONALES DE LOS MENORES Y NUEVOS DERECHOS DIGITALES

## 1. Introducción

En las últimas décadas, existe especial preocupación sobre el contenido, la importancia y el desarrollo del derecho a la protección de datos de la niñez y la adolescencia. Las redes sociales "alojan enormes cantidades de datos personales de sus usuarios que, a través de sus perfiles personales, aportan y publican constantemente información e imágenes sobre ellos mismos e, incluso, sobre terceros (amigos, familiares o hijos menores de edad), sin el consentimiento de éstos"[1]. Así, el debate se plantea en precisar las condiciones y mecanismos de control que supone el tratamiento de datos en entornos digitales.

En la era digital, el tratamiento de datos exige la adopción de medidas de protección adecuadas, preventivas y pertinentes que –en el ámbito del Estado, la sociedad y la familia– aseguren un equilibrio, entre el libre flujo de la información y la privacidad de los datos de las personas, especialmente, de los menores. Por ejemplo, queremos destacar la privacidad por defecto y la privacidad desde el diseño, las cuales suponen "un cambio para los menores ya que ellos no tienen la madurez necesaria para pensar en el valor de sus datos de carácter personal y en el carácter oneroso de los proveedores de las Redes Sociales y de las demás herramientas de Internet"[2]. Estos deberes que plantea el escenario de modernidad de las tecnologías es, en principio, complejo por la variedad de exigencias, políticas, deberes y responsabilidades que el Estado, la sociedad y la familia deben asumir para materializar la seguridad y la confianza ciudadana.

[1] Pablo García Mexia y Carmen Perete Ramírez, "Internet y el Reglamento General de Protección de Datos", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 176.

[2] Laura Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. Madrid. Agencia Española de Protección de Datos. 2017, 31.

El derecho a la protección de datos es un derecho nuevo que pertenece a las últimas generaciones de derechos, "es decir, las formadas por aquellos que responden a los retos y dificultades de la sociedad de nuestros días. Principalmente, a los derivados del avance tecnológico, del impacto sobre el medio y de las nuevas formas de desigualdad"[3]. En la sociedad de la información, a partir, de las dificultades que plantean el uso y la aplicación de las tecnologías de la información y comunicación (Tics), la comunidad internacional ha expresado una constante preocupación por la protección de datos, especialmente, en entornos en los que pueden verse comprometidos la vida privada, el desarrollo de la personalidad y la dignidad de las personas.

En el caso de los menores, sus derechos exigen adoptar cuidados y mecanismos especiales de protección, que aseguren el pleno disfrute y desarrollo de su personalidad[4] . No es desconocido que el derecho a la identidad se encuentra, especialmente, incardinado con el derecho a la vida privada y al principio de autonomía de la persona[5]. Todos ellos garantes de la protección de la dignidad humana que exigen la adopción de medidas especiales, por el grado de vulnerabilidad al que pueden verse expuestos los menores. Por tanto, siendo uno de los derechos de personalidad el derecho a la identidad, el cual comprende una serie de atributos y características que permite la identificación y/o individualización de las personas; entendemos que la identidad de la persona puede afectarse a consecuencia de un sinfín de contextos, entre ellos Internet y redes sociales.

Bajo estas consideraciones, en esta parte, abordaremos algunas consideraciones sobre la protección de la información de carácter personal de los menores y los nuevos derechos digitales que los tutelan. Este planteamiento sugiere hacer una aproximación al concepto de datos personales de los menores en la sociedad de información, y así también conceptualizar el papel de la familia, frente a las

[3] Pablo Lucas Murillo de la Cueva y José Luis Piñar Mañas, El *derecho a la autodeterminación informativa* (Madrid-México: Fontamara S.A, 2011), 14.
[4] Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-17/2002 relativa a la condición jurídica y derechos humanos del niño, solicitada por la Comisión Interamericana de Derechos Humanos. 2002.
[5] Cfr. Caso Artavia Murillo y otros Vs. Costa Rica, Sentencia de 28 de noviembre de 2008. párr.143.

innumerables amenazas que se presentan como ofensivas para la privacidad e identidad digital en plataformas digitales, principalmente, redes sociales. Si bien corresponde enfatizar en la necesidad de garantías normativas que hagan posible ejercer, equilibradamente, el derecho a la protección de datos en la sociedad, nuestra intención es precisar las medidas y deberes de protección que la familia debería adoptar para asegurar los derechos de los menores, en la era de la modernidad tecnológica[6].

Para este fin, la normativa internacional desarrollada, en la Unión Europea y en la Comunidad Andina, significa el referente para cristalizar un modelo de cultura digital que la protección de datos requiere para afianzar los presupuestos jurídicos de tutela y corresponsabilidad[7]. Lógicamente, el Reglamento (UE) 2016/679, los EPEI y el Memorándum de Montevideo, para la protección de datos personales y la vida privada en las redes sociales en Internet, referenciarán los principios que deben considerarse como prioritarios para enfrentar los riesgos que suponen las Tics –especialmente, Internet y redes sociales digitales–, frente al tratamiento de la información personal en entornos digitales.

[6] Bajo este supuesto, la Corte Interamericana de Derechos Humanos enfatiza en la protección a la familia por ser "el lugar por excelencia donde deben efectivizarse en primer lugar los derechos de los niños, las niñas y los adolescentes cuyas opiniones deben ser priorizadas para la toma de decisiones familiares". Por tanto, "corresponde al Estado precisar las medidas que adoptará para alentar ese desarrollo en su propio ámbito de competencia y apoyar a la familia en la función que ésta naturalmente tiene a su cargo para brindar protección a los niños que forman parte de ella. Tal como se señalan en las discusiones de la Convención sobre los Derechos del Niño, es importante destacar que los niños poseen los derechos que corresponden a todos los seres humanos –menores y adultos– y tienen además derechos especiales derivados de su condición, a los que corresponden deberes específicos de la familia, la sociedad y el Estado". Cfr. Corte Interamericana de Derechos Humanos. Opinión consultiva OC-17/2002 relativa a la condición jurídica y derechos humanos del niño, solicitada por la Comisión Interamericana de Derechos Humanos. 2002.

[7] Así, pretendemos considerar las bases para articular y promover una "cultura digital", como mecanismo de prevención que, sustentado en la corresponsabilidad, integre los derechos y deberes que corresponden al derecho a la protección de datos en los menores.

## 2. Los entornos digitales y el cambio de paradigma en la protección de datos personales

Considerando que el derecho a la protección de datos tiene una gran connotación, desde el ámbito tecnológico, en una sociedad en red, este derecho comporta, además, un conjunto de facultades destinadas a garantizar el control, el dominio de la información personal y la intimidad de las personas. Por ello, "es necesario que el Derecho no permanezca ajeno a esta realidad y que, en todo caso, las personas, organismos, organizaciones y entidades que estén en contacto directo con los menores tengan conocimiento de esta realidad y prevean mecanismos de actuación para implementarlos en caso de que sea necesario"[8]. En todo caso, frente a la pérdida de sensibilidad de compartir información personal de los menores, en entornos digitales, entendemos que "esa forma de intimidad no se concibe como un valor intrasubjetivo, sino como autodeterminación del sujeto en el seno de sus relaciones con los demás ciudadanos y con el poder público"[9].

Según la UNESCO, la sociedad del conocimiento y de la información debe procurar el desarrollo humano sostenible. Ante este supuesto, las Tics plantean serias dificultades para el desarrollo de la sociedad en lo que se refiere al respeto de derechos, por terceros, relacionados con la dignidad, intimidad, privacidad, entre otros bienes jurídicos, dentro de entornos digitales. Por tanto, en lo que refiere a la protección de datos, hay que recordar que este derecho fundamental nace, no solamente de la exigencia a terceros sino también de la autodeterminación del propio sujeto que es el titular de los datos personales. Así, en primer término, advertimos una permanente falta de conciencia de las personas "sobre las implicaciones que para su privacidad pueden derivarse del uso de las redes sociales. Esta falta de conciencia se debe a que, frecuentemente, las Políticas de Privacidad de estas plataformas no explican con claridad qué datos se recogen, para qué van a ser tratados, con qué otros datos se van a combinar y a quiénes se

[8] Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. 54.
[9] Enrique Pérez-Luño Robledo, *El procedimiento de Habeas data: El derecho procesal ante las nuevas tecnologías***,** (Madrid: Editorial Dykinson S.L, 2017), 104.

van a comercializar"[10]. Al parecer, la sociedad no es consciente de los riesgos que supone compartir información personal propia y de terceros, sin el consentimiento de aquellos. Tampoco es consciente de la normativa que impide que existan intromisiones ilegitimas en la vida privada de las personas.

En este marco, corresponde subrayar que debe imponerse "un diálogo entre la regulación normativa y la autorregulación, entre la protección de datos como derecho fundamental (…) y como criterio para el tratamiento de datos y compromiso por parte de quienes lo manejan"[11]. Desde esta perspectiva, consideramos que:

> La privacidad no trata solo del respeto a nuestros datos personales sino también del que debemos tener por la información relativa a los demás. Una característica de las redes sociales –y, más en general, de la web 2.0- es que son los usuarios los que incorporan la información personal. Estos tienen que respetar los derechos de los demás y no publicar información de otros –por ejemplo, fotografías- sin autorización[12].

Si bien, el derecho a la protección de datos afecta al común de las personas y la sociedad en general, esta característica precisa también mayor atención en la niñez y adolescencia. Tomando en cuenta que –por ejemplo, en Ecuador–, la niñez y adolescencia es considerado como un grupo de atención prioritaria; la protección de este derecho debe ejercerse sobre la base del principio de interés superior del niño, en donde los padres tienen "un deber preventivo (formación) y un deber reactivo (actuación en caso de ataques por parte de terceros). Ambos deberes han de estar en el justo equilibro en la balanza con los derechos de los menores de protección de datos"[13]. De esta forma, la protección de la información personal de los menores tiene particular importancia, toda vez, que los riesgos que traen consigo los entornos digitales representan una amenaza dentro del tratamiento de datos.

> Poco a poco, las redes sociales van generando y almacenando un archivo de cada usuario con todos los datos que ha facilitado desde que se dio de alta en la red social, a los que se van añadiendo los comentarios que publican sobre sus aficiones, trabajos, amistades, actividades, viajes, fotos, etc. Toda esta información que se facilita, tantas veces de manera

[10] García Mexia y Perete Ramírez, "Internet y el Reglamento General de Protección de Datos", 177.
[11] Lucas Murillo de la Cueva y Piñar Mañas, El *derecho a la autodeterminación informativa*, 179.
[12] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1714**.**
[13] Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. 72.

inconsciente y despreocupada, sirve para ir configurando un perfil cada vez más definido del usuario[14].

En presencia de esta situación "es especialmente grave la posibilidad que ofrecen las redes sociales para llevar a cabo el *cyberbullying* –acoso a través de las tecnologías de la información–, que convierte la vida de algunos jóvenes o de profesores en una auténtica pesadilla"[15]. En todo caso, consideramos que, además, "muchos de los atentados a los datos personales de menores, así como determinados acosos contra su libertad, su integridad o su imagen, tienen como autores a otros niños"[16]. En efecto, el *cyberbullying* "suele tener lugar en entornos escolares —colegios, institutos, escuelas de formación profesional— y deja una huella psicológica en la víctima. En esta situación, hay un menor que actúa como víctima y uno —o varios— menores que actúan como verdugos"[17].

El uso de tics –principalmente, en la niñez y la adolescencia–, es una de las características del siglo XXI a nivel mundial. En un sentido, estrictamente, positivo, su objeto está orientado a hacer desaparecer la brecha y analfabetismo digital en la sociedad. No obstante, en un sentido negativo, las tecnologías –por ejemplo, mediante el uso de redes sociales– "permiten desarrollar conductas hostiles, atacar la reputación, dañar la intimidad de otras personas a través de comentarios, invención de historias, creación de perfiles falsos, suplantación de la personalidad, etiquetado de fotos, etc."[18]. En los últimos años, en la sociedad del conocimiento y de la información, uno de los principales objetivos de los Estados ha sido masificar en la población el acceso y uso de las Tics[19]. En el informe de 2019 publicado por *We Are Social*, "a nivel mundial, los usuarios de Internet crecieron un 8,6 por ciento

[14] García Mexia y Perete Ramírez, "Internet y el Reglamento General de Protección de Datos", 177.
[15] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1714.
[16] Pérez-Luño Robledo, *El procedimiento de Habeas data,* 186.
[17] Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. 50.
[18] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1714-1715**.**
[19] Por ejemplo, uno de los objetivos de desarrollo sostenible (ODS) de la Organización de las Naciones Unidas (ONU) es "construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación". Entre las metas del objetivo 9, precisamente, destaca "aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados".

en el último año, con 350 millones de nuevos usuarios que contribuyeron a un total de 4.437 mil millones"[20]. Así también, en un estudio de la UNICEF se señala que "los jóvenes (de 15 a 24 años) son el grupo de edad más conectado. En todo el mundo, el 71% están en línea, en comparación con el 48% de la población total (…) Los niños y adolescentes menores de 18 años representan aproximadamente uno de cada tres usuarios de Internet en todo el mundo"[21].

La relación, entre la tecnología y el derecho a la protección de datos, es una cuestión que no puede pasar desapercibida. Este derecho fundamental se considera como un instituto de garantía que exige el respeto, en sociedad, "de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento"[22]. Por ello, su protección "tiene una importancia decisiva en las sociedades tecnológicas del presente. Su función se cifra en garantizar a los ciudadanos unas facultades de información, acceso y control de los datos que les conciernen"[23]. A partir del uso de las Tics por la niñez y la adolescencia, existe coincidencia en denominar a éstos como nativos digitales, en virtud de su acercamiento con el uso de las Tics a edades, relativamente, tempranas. Algunos datos coinciden en esta afirmación cuando, por ejemplo, se menciona que en Estados Unidos el 92% de los menores tienen una identidad digital

[20] Además, este informe observa que "ahora hay más de 5,1 mil millones de personas en el mundo que usan un teléfono móvil, un aumento anual del 2,7 por ciento, y los teléfonos inteligentes representan más de dos tercios de todos los dispositivos en uso en la actualidad". Cfr. Simon Kemp, *Global Digital Report in 2019*. Disponible en: https://tinyurl.com/y3cjyn69. El informe de 2018 concluyó que "más de la mitad de la población mundial ahora está en línea, y los últimos datos muestran que casi 250 millones de nuevos usuarios se conectaron por primera vez en 2017". Cfr. Simon Kemp, *Global Digital Report in 2018*. Disponible en: https://tinyurl.com/y4otyg4b.

[21] Cfr. Unicef (Fondo de las Naciones Unidas para la Infancia), "*El Estado Mundial de la Infancia 2017: Niños en un mundo digital*". Disponible en: https://www.unicef.org/spanish/sowc2017/.

[22] Artemi Rallo Lombarte, "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)", *UNED: Revista de Derecho Político*, Nro. 100 (2017), 639-669.

[23] Pérez-Luño Robledo, *El procedimiento de Habeas data,* 104.

a los dos años[24]. Esta realidad no es diferente a nivel mundial. Como agrega la UNICEF en su informe:

> La infancia no es una excepción. Desde el momento en que cientos de millones de niños llegan al mundo, están inmersos en una corriente constante de comunicación y conexión digitales, desde la forma en que se gestiona y brinda su atención médica hasta las imágenes en línea de sus primeros momentos más preciosos[25].

En el caso de Ecuador en 2016, según datos del Instituto Nacional de Estadísticas y Censos (INEC), el 63.4 % de niños entre 5 a 15 años usaron Internet, y así también 8 de cada 10 jóvenes entre 16 y 24 años con un 78.9%[26]. De esta manera, los niños representan la segunda franja etaria con mayor número de personas que utiliza computadora, incrementándose desde el 2012 un 18,2% el uso de Internet en los más pequeños, y, además un 55.9% el uso de *smarphones* dentro de los últimos cinco años[27]. Desde esta perspectiva, es fundamental centrarse en los presupuestos que deben converger hacia una tutela efectiva de los derechos derivados del uso de las tecnologías, particularmente, del derecho a la protección de datos. "Entre otros, los principios de información, transparencia, finalidad, consentimiento y responsabilidad, siguen siendo la clave para garantizar la protección de datos personales o la privacidad e impulsar la confianza necesaria en la innovación"[28]. En el caso de los menores, la corresponsabilidad presenta un valor agregado, puesto que, a efectos de concretar el anhelado equilibrio en la protección de datos, es un presupuesto que no debe tratarse de forma aislada.

---

[24] Paula Otero, "Sharenting… ¿la vida de los niños debe ser compartida en las redes sociales?", *Arch Argent Pediatr,* (2017): 412-413.

[25] Cfr. Unicef (Fondo de las Naciones Unidas para la Infancia), "*El Estado Mundial de la Infancia 2017: Niños en un mundo digital*".

[26] Datos extraídos de la página web del Instituto Nacional de Estadísticas y Censos (INEC), en relación al estudio de 2016 sobre "Las Tecnologías de la Información y Comunicación (TIC) – 2016", para el análisis y formulación de políticas públicas. Disponible en: https://tinyurl.com/y8epe5ub. Este estudio comprendió a grupos definidos entre 5 a 15 años; 16 a 24 años; 25 a 34 años; 35 a 44 años; 45 a 54 años; 55 a 64 años; y 65 años.

[27] Cfr. La infografía del estudio de 2016, sobre "Las Tecnologías de la Información y Comunicación (TIC) – 2016" para el análisis y formulación de políticas públicas. Disponible en: https://tinyurl.com/yy7vtacu.

[28] Miguel Recio Gayo, *Protección de datos personales e Innovación: ¿(In) compatibles?* (Madrid: Reus, 2016), 16.

Así pues, sustentados en la corresponsabilidad, la idea de un modelo de cultura digital para la protección de datos no es un paradigma que deba desatenderse, ya que, como advierte el informe *We are Social*, "aproximadamente el 98 por ciento de los usuarios de redes sociales del mundo, más de 3.400 millones de personas, acceden a plataformas sociales a través de dispositivos móviles"[29]. Así también, el informe de la UNICEF subraya que 1 de cada 3 usuarios de Internet son niños. Por tanto, "la acción, por parte de los gobiernos, las organizaciones internacionales, la sociedad civil, los centros de enseñanza, el sector privado y las familias, los niños y los jóvenes, debe coincidir con el ritmo del cambio"[30].

Hasta aquí, no pretendemos presentar un panorama desalentador sobre el uso de las tecnologías. Al contrario, nuestro objetivo es indicar las medidas necesarias que fundamenten un modelo de cultura digital. Un modelo que armonice el uso de las Tics y vincule a éstas con el respeto de la dignidad humana, frente al derecho a la protección de datos en entornos digitales, por cuanto, "la solución no está en limitar la utilización de las tecnologías de la información y de las comunicaciones, sino en hacer compatible su desarrollo con los derechos de los ciudadanos"[31]. Para alcanzar este fin, según el Memorándum de Montevideo, un elemento esencial es la prevención y la corresponsabilidad. Conjuntamente, al ámbito normativo, judicial y de políticas públicas, estos supuestos permitirán posibilitar la concienciación en los usuarios sobre los riesgos que implique compartir datos personales relativos a menores[32].

---

[29] Cfr. Kemp, Simon. *Global Digital Report in 2019*.

[30] Cfr. Unicef (Fondo de las Naciones Unidas para la Infancia), "*El Estado Mundial de la Infancia 2017: Niños en un mundo digital*". Al constituir el primer y único informe de la UNICEF sobre los efectos del uso de la tecnología digital en la vida de los niños, este estudio representa en la actualidad una oportunidad en el objetivo de equilibrar, consensuar y conciliar el uso de las Tics con el respeto de la dignidad humana y, en particular, con el derecho a la protección de datos de los menores.

[31] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 35.

[32] El "Memorándum de Montevideo", sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, se trata de un documento que adopta una serie de recomendaciones dentro del Seminario de trabajo realizado en Montevideo los días 27 y 28 de julio de 2009. Fue convocado por el Centro Internacional de Investigaciones para el Desarrollo de Canadá, en donde se concentraron los principales representantes gubernamentales de Brasil, Canadá, España, Uruguay, Perú, Ecuador, Colombia, Argentina y México. Teniendo como referente normativo a la Convención de Naciones Unidas sobre los Derechos del Niño (CDN), su

En este marco, los EPEI refieren que la niñez y la adolescencia requiere garantías adecuadas –entre ellas la formación académica– que permitan concienciar sobre "el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación" –art. 8.2–. Además, tomando en cuenta que el RGPD considera que el desarrollo de las tecnologías ha llegado a transformar, tanto la economía como la vida en la sociedad, en el caso de los derechos relativos a la niñez señala que estos "merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales" –Considerando 38–. Además, según la LOPDGDD, la garantía de los derechos digitales de los menores constituye uno de los aspectos más importantes, por cuanto en su contenido evidenciamos una serie de disposiciones relacionadas con la protección del menor en Internet.

El desarrollo de las tecnologías debe mirarse como una oportunidad, frente a la libre circulación de datos. "La búsqueda de este equilibrio requiere tener presentes todos los aspectos que se plantean, tanto sociales, como económicos, jurídicos, políticos y tecnológicos"[33]. Naturalmente, dentro del aspecto social, un papel relevante lo cumple la familia, como el núcleo central, donde los menores fortalecerán su imagen y responsabilidad en el mundo virtual. En todo caso, a la hora de garantizar la tutela del derecho a la protección de datos de los menores, todos estos aspectos requieren que los padres adopten las necesarias medidas de protección de la información personal de sus hijos, frente a la evolución del fenómeno informático.

> En primer lugar, es necesario que los padres asuman como propia la labor de «formación en TIC» de sus hijos. Partiendo de esto, el primer consejo a poner en práctica es que eviten hacer de sus hijos «huérfanos digitales». Con esta expresión nos referimos a aquellos «nativos digitales» que no cuentan con el apoyo de sus padres. Y es que, si bien es cierto que, en muchas ocasiones, los hijos manejan con mayor soltura que sus progenitores las

principal objetivo fue exponer las problemáticas derivadas de la protección de los derechos fundamentales de los niños, niñas y adolescentes, a partir, de los riesgos que suponen la Sociedad de la Información y Conocimiento. Tal como se señala en este documento, las recomendaciones formuladas son "una contribución para que los diversos actores involucrados de la región se comprometan con el tema para extender los aspectos positivos de la Sociedad de la Información y Conocimiento, incluyendo Internet y las redes sociales digitales, así como prevenir aquellas prácticas perjudiciales que serán muy difíciles de revertir, así como los impactos negativos que las mismas conllevan". Cfr. Memorándum de Montevideo. Disponible en: http://www.iijusticia.org/Memo.htm.

[33] Recio Gayo, *Protección de datos personales e Innovación: ¿(In) compatibles?,* 16.

> herramientas tecnológicas, también lo es que los menores no cuentan con una «cultura digital» suficiente para conocer los riesgos de estas herramientas y es ahí donde los padres juegan un papel fundamental para que su hijo no sea un «huérfano digital» sino un «nativo digital consciente y formado», haciendo hincapié en este sentido en que no se trata sólo de ofrecerle formación sobre los riesgos, amenazas y peligros que supone el uso de las TIC sino también de las innumerables ventajas y beneficios que le puede reportar un uso correcto de estas herramientas[34].

La privacidad y la seguridad en línea de los menores están en juego. Es evidente la necesidad de buscar un equilibrio normativo global, que garantice la protección integral de la información personal en el mundo digital. La responsabilidad de cuidar los propios datos personales es un presupuesto que, no solamente obliga a terceras personas sino también a los propios titulares de los datos. En este contexto, puede decirse que la normativa internacional antes expuesta, nos permitirá señalar las bases para promover, particularmente, en la niñez y la adolescencia, una cultura digital que –sustentada en la corresponsabilidad–, garantice el derecho a la protección de datos.

Desde otra perspectiva, gran parte de la solución está en la educación, "una labor que corresponde no sólo a los profesores sino especialmente a los padres y que contribuirá a encontrar un equilibrio entre el deseo de comunicación y de ampliación del círculo de amistades y el respeto a la dignidad de la persona en Internet[35]. Los padres y, en suma, las familias deben enseñar a los hijos "la importancia del respeto como principio básico de comportamiento —tanto a uno mismo como a los demás— ya sea en el ámbito *offline* como en el *online*, pudiéndose seguir en este punto la máxima de «Tratar a los demás como te gustaría que te trataran a ti»"[36].

Ahora bien, el concepto de corresponsabilidad, en materia de protección de datos, nace del deber que se impone al Estado, la sociedad y la familia. Se encamina a adoptar medidas –sociales, políticas y jurídicas– para la plena vigencia, ejercicio, garantía, protección y exigibilidad de los derechos de los titulares de la información.

---

[34] Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. 74.
[35] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1719.
[36] Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. 75.

> Una estrategia eficaz, en este contexto, puede ser la formulación de acuerdos entre las Agencias de Protección de Datos, Ministerios de Educación y otros organismos responsables, definiendo condiciones claras y prácticas de cooperación mutua en esta área para fomentar la noción de que la protección de datos es un derecho fundamental[37].

Sin embargo, en la práctica todo parece apuntar a que –por ejemplo, en el caso de la niñez y la adolescencia–, éstos se encontrarían en cierto estado de "orfandad digital", frente al uso de las tecnologías. Como agrega el informe de la UNICEF:

> Las lagunas en nuestro conocimiento sobre la vida de los niños en línea, incluidas las repercusiones de la conectividad sobre la cognición, el aprendizaje y el desarrollo social y emocional, dificultan la elaboración de políticas dinámicas que superen los problemas abordando los riesgos y aprovechando al máximo las oportunidades. Las lagunas en nuestra comprensión sobre la manera en que los niños consideran su experiencia de conectividad, incluidas sus percepciones de los riesgos, nos limitan aún más[38].

Todo este escenario conlleva a la realización de un análisis sobre la necesidad de contar con modelos conducentes, los cuales afiancen una cultura digital del derecho a la protección de datos, particularmente, para la niñez y la adolescencia materializados, por ejemplo, a través de la corresponsabilidad de la familia y de la aplicación de políticas públicas.

## 3. La corresponsabilidad: El papel de la familia

La protección de datos de los menores se afianza en el principio constitucional de interés superior del menor, previsto en el art. 44, por el cual se precisa una especial observancia de la niñez y la adolescencia[39]. A la familia le corresponde que "adopten medidas encaminadas a la formación del menor en TIC y a la prevención de que

[37] Pérez-Luño Robledo, *El procedimiento de Habeas data,* 190.

[38] Cfr. Unicef (Fondo de las Naciones Unidas para la Infancia), "*El Estado Mundial de la Infancia 2017: Niños en un mundo digital*".

[39] En Ecuador el principio de interés superior del niño, además, se encuentra reconocido en el art. 11 del Código de la Niñez y la Adolescencia. Está orientado a satisfacer "el ejercicio efectivo del conjunto de los derechos de los niños, niñas y adolescentes; e impone a todas las autoridades administrativas y judiciales y a las instituciones públicas y privadas, el deber de ajustar sus decisiones y acciones para su cumplimiento. Para apreciar el interés superior se considerará la necesidad de mantener un justo equilibrio entre los derechos y deberes de niños, niñas y adolescentes, en la forma que mejor convenga a la realización de sus derechos y garantías. Este principio prevalece sobre el principio de diversidad étnica y cultural. El interés superior del niño es un principio de interpretación de la presente Ley. Nadie podrá invocarlo contra norma expresa y sin escuchar previamente la opinión del niño, niña o adolescente involucrado, que esté en condiciones de expresarla".

puedan ser víctimas de ciberataques o de otros inconvenientes del uso de las Redes Sociales"[40]. Frente a la vida privada de los menores, la evolución de las tecnologías ha llegado a significar una potencial amenaza para la protección y defensa de sus derechos fundamentales[41]. Conflictos jurídicos que resultan de actos de odio, discriminación, extorsión y acoso sexual representan, solamente, algunos de los principales peligros en una sociedad en que la información personal –todo aquello que pueda identificar o hacer identificable a una persona– requiere especial atención por la sobrexposición a la que pueden ser sujetos.

Como sabemos, los datos personales revelan aquellas características, aspectos y cualidades innatas que corresponden a la individualidad y personalidad de un individuo[42]. Tomando en cuenta el acelerado avance de las tecnologías, existe una preocupación por la protección de los datos, "ya que éstas tienen una gran capacidad para recoger datos personales, grabarlos, ponerlos en comunicación y hacer transferencias internacionales, permitiendo los tratamientos masivos de información personal, por lo que representan las mayores injerencias en este derecho fundamental"[43]. Como señala Lucas Murillo de la Cueva, "la dimensión universal que han alcanzado las relaciones sociales gracias a las redes que superan las fronteras estatales ha llevado a buscar soluciones también universales para hacer efectiva la protección de datos de carácter personal"[44].

Nos parece que, además de buscar soluciones universales enmarcadas en marcos jurídicos homogéneos, es la hora de equilibrar el derecho a la protección de datos, a partir de las funciones que cumple la familia. Como determina la Constitución de

---

[40] Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. 76.

[41] No es desconocido el riesgo que trae el uso de las tecnologías. Si en esta relación se encuentran involucrados menores, las Tics convierten a éstos, en unos casos, en blanco fácil para quienes se aprovechan de la información personal registrada en la web, dando lugar al "*Grooming*", "*Morphing*" etc.; y en otros casos, caracterizan situaciones cotidianas que –por el mal uso de la información personal– desencadenan en afectaciones a la imagen, honor y dignidad de la persona, mediante el "*Sexting*", "*Ciberbullying*" etc.

[42] Por ejemplo, una imagen, la dirección correo electrónico, número de cédula, dirección domiciliaria, dirección IP; y otros datos, considerados como especialmente protegidos, como las creencias religiosas, ideología política, convicciones morales y condiciones de salud personal.

[43] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 32.

[44] Pablo Lucas Murillo de la Cueva, "La protección de los datos de carácter personal en el horizonte de 2010", Anuario Facultad de Derecho – Universidad de Alcalá Navarra. Nro. ll. 2009, 133.

Ecuador, el Estado “promoverá la corresponsabilidad materna y paterna y vigilará el cumplimiento de los deberes y derechos recíprocos entre madres, padres, hijas e hijos” –art. 69.5–. Éste es un deber y una responsabilidad de los progenitores en igual proporción, respecto a “asistir, alimentar, educar y cuidar a las hijas e hijos” –art. 83.16–. Así también según el Código de la Niñez y la Adolescencia, el concepto de corresponsabilidad advierte que es deber del Estado, la sociedad y la familia, “dentro de sus respectivos ámbitos, adoptar las medidas políticas, administrativas, económicas, legislativas, sociales y jurídicas que sean necesarias para la plena vigencia, ejercicio efectivo, garantía, protección y exigibilidad de la totalidad de los derechos” –art. 8–. En este punto, también este cuerpo normativo determina que la familia constituye “el espacio natural y fundamental para el desarrollo integral del niño, niña y adolescente. Corresponde prioritariamente al padre y a la madre, la responsabilidad compartida del respeto, protección y cuidado de los hijos y la promoción, respeto y exigibilidad de sus derechos” –art. 9–.

Las condiciones necesarias para el ejercicio y protección de los datos personales en la niñez y la adolescencia, se derivan de los derechos comunes al ser humano y de las libertades determinadas en el ordenamiento jurídico constitucional[45]. En todo caso, considerando que el art. 11.3 de la Constitución reconoce los derechos y garantías establecidos en los instrumentos internacionales, hay que estimar la importancia de aquellos que en materia de menores desarrollan el contenido de sus derechos. Así, frente a las condiciones que corresponden a la familia, en la tarea de concretar un modelo de corresponsabilidad en la protección de datos de los menores, en entornos digitales, un importante instrumento internacional constituye la Opinión Consultiva 17/2002, solicitada por la Comisión Interamericana de Derechos Humanos, por la cual la CIDH establece la “Condición Jurídica y Derechos Humanos del Niño”.

[45] Tal como señala la Constitución de Ecuador, “las niñas, niños y adolescentes gozarán de los derechos comunes del ser humano, además de los específicos de su edad” –art. 45–. Así también el Código de la Niñez y la Adolescencia establece que “los niños, niñas y adolescentes son sujetos de derechos y garantías y, como tales, gozan de todos aquellos que las Leyes contemplan en favor de las personas, además de aquellos específicos de su edad” –art. 15–.

La CIDH conceptualiza a la familia como el núcleo central de protección y la define como “el ámbito primordial para el desarrollo del niño y el ejercicio de sus derechos”[46]. En la era digital, esta definición conlleva el aseguramiento de un desarrollo equilibrado, de tal manera, que su información personal no sea objeto de intromisiones ilegales y/o arbitrarias. Por esta razón, el papel de la familia es fundamental “en el proceso de educación sobre el uso responsable y seguro de herramientas como Internet y las redes sociales digitales y en la protección y garantía de sus derechos”[47]. Las medidas especiales para la protección de los derechos de privacidad, datos personales y de identidad digital exigen condiciones relacionadas con la concienciación, educación, control y supervisión, que aseguren prácticas responsables de Internet y redes sociales. Por ello, en esta parte, lo que intentaremos es resaltar la importancia de proteger la identidad digital de los menores.

En efecto, la identidad digital debe ser el bien jurídico protegido, ante la interacción de éstos en las redes sociales; identidad digital que han de tener presente que se configura como una potestad de quien no tiene la mayoría de edad de dar a conocer aspectos personales e íntimos, a veces, difundiendo fotos, videos, o a través de comentarios[48]. Por ello, insistimos en que, en materia de protección de datos, las garantías de tutela, necesariamente, deben converger con las obligaciones que supone el ejercicio de la patria potestad de los padres, con el objeto de garantizar el cuidado y el desarrollo integral de los menores. En suma, asegurar la tutela efectiva de su derecho a la identidad digital.

[46] Sobre esta definición, la CIDH enfatiza en que “la familia es la unidad central encargada de la integración social primaria del niño, los gobiernos y la sociedad deben tratar de preservar la integridad de la familia, incluida la familia extensa. La sociedad tiene la obligación de ayudar a la familia a cuidar y proteger al niño y asegurar su bienestar físico y mental”. Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-17/2002 relativa a la condición jurídica y derechos humanos del niño, solicitada por la Comisión Interamericana de Derechos Humanos.2002.

[47] Véase, Memorándum de Montevideo, 2009.

[48] Cfr. Ángel Acedo y Alejandro Platero, “La privacidad de los niños y adolescentes en las redes sociales: Referencia especial al régimen normativo europeo y español, con algunas consideraciones sobre el chileno”, *Revista Chilena de Derecho y Tecnología,* Nro. 5 (2016): 63-94.

Por otra parte, hay que comprender que "la violación a la privacidad, incluida la divulgación de datos personales como fotografías e identidades de los niños, puede servir para explotarlos, algo que podría generar graves consecuencias"[49]. Como advierte la CIDH, "la familia debe proporcionar la mejor protección de los niños contra el abuso, el descuido y la explotación. Y el Estado se halla obligado no sólo a disponer y ejecutar directamente medidas de protección de los niños sino también favorecer, de la manera más amplia, el desarrollo y la fortaleza del núcleo familiar[50]. Con referencia a este aspecto, resaltamos que "en todo el mundo se han creado numerosas campañas nacionales para crear conciencia sobre los problemas de seguridad de Internet, alentar el comportamiento responsable en línea y promover el cambio de políticas"[51]. En este orden, la familia cumple un papel trascendental en el aseguramiento de la protección de los datos de los menores[52]. Por tanto, advertimos que el deber de garantizar este derecho fundamental –y, en suma, el derecho a su identidad digital–, no solamente es exigible al Estado y la sociedad.

Con frecuencia decimos que "la familia es la primera escuela" y, consecuentemente, la tutela de estos derechos y bienes jurídicos deben proveerse también en gran medida de prohibiciones y mecanismos de control parental. De este modo, "en la misma línea de convertirse en un ejemplo para sus hijos seguimos al instar a los padres a registrarse en la misma red social que su hijo de manera que conozcan de primera mano las funcionalidades de la red y el potencial de la plataforma"[53]. En todo caso, frente al uso de estas redes, advertimos que, en el caso de los menores

[49] Cfr. Unicef (Fondo de las Naciones Unidas para la Infancia), "*El Estado Mundial de la Infancia 2017: Niños en un mundo digital*", 68.
[50] Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-17/2002 relativa a la condición jurídica y derechos humanos del niño, solicitada por la Comisión Interamericana de Derechos Humanos.2002.
[51] Cfr. Unicef (Fondo de las Naciones Unidas para la Infancia), "*El Estado Mundial de la Infancia 2017: Niños en un mundo digital*", 86.
[52] En este sentido, destacamos un triple deber que, como advierte la CIDH, "corresponde tanto al Estado como a la familia, la comunidad y la sociedad a la que aquél pertenece" Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-17/2002 relativa a la condición jurídica y derechos humanos del niño, solicitada por la Comisión Interamericana de Derechos Humanos.2002.
[53] Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. 75.

"se deberá considerar la prohibición de tratamiento de datos personales", mientras que en el caso de los adolescentes "se deberá tener en cuenta los mecanismos de controles parentales, de los que deben darse una información clara"[54].

La aparición de nuevas tecnologías como Internet y redes sociales representan un cambio de paradigma en la protección de los datos, de la intimidad, la privacidad e identidad digital de las personas. En el caso de los menores, este escenario plantea en la familia nuevas problemáticas y tensiones. Por ello, los padres y quienes forman parte del vínculo familiar tienen la obligación de "conocer que existen riesgos en el hecho de compartir información sobre sus hijos en las redes sociales. Entre los daños que pueden suceder, se encuentra el robo de identidad y que se compartan imágenes en sitios que fomentan la pedofilia"[55]. De esta forma, las garantías y mecanismos de control para la protección de los datos personales en la niñez y adolescencia, deben enmarcarse en el principio de interés superior, lo cual supone "que el desarrollo de éste y el ejercicio pleno de sus derechos deben ser considerados como criterios rectores para la elaboración de normas y la aplicación de éstas en todos los órdenes relativos a la vida del niño"[56]. En este contexto y, sobre la base de este principio, "la protección de la privacidad de los niños y jóvenes en Internet está suscitando un enorme debate y, fruto de ello, gran cantidad de iniciativas internacionales pretenden aumentar el nivel de protección de estos derechos del niño"[57].

[54] Véase, Memorándum de Montevideo, 2009.
[55] Otero, "Sharenting… ¿la vida de los niños debe ser compartida en las redes sociales?", *Arch Argent Pediatr,* 413.
[56] Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-17/2002 relativa a la condición jurídica y derechos humanos del niño, solicitada por la Comisión Interamericana de Derechos Humanos.2002. En este caso, la CIDH agrega que "este principio regulador de la normativa de los derechos del niño se funda en la dignidad misma del ser humano, en las características propias de los niños, y en la necesidad de propiciar el desarrollo de éstos, con pleno aprovechamiento de sus potencialidades, así como en la naturaleza y alcances de la Convención sobre los Derechos del Niño".
[57] Acedo y Platero, "La privacidad de los niños y adolescentes en las redes sociales: Referencia especial al régimen normativo europeo y español, con algunas consideraciones sobre el chileno", 65.

Las referencias citadas en torno a la invasión de la privacidad en entornos digitales y los riesgos a los que se exponen exigen de la familia garantías, para el ejercicio pleno de los derechos de los menores en todos los órdenes. Los mecanismos de control de la información personal deben priorizar "el interés superior de niñas, niños y adolescentes, guardando un equilibrio entre las necesidades de protección contra la vulneración de sus derechos y el uso responsable de esas herramientas que representan formas de ejercicio de sus derechos"[58]. En este marco, además, la actividad del Estado es primordial, a efecto de asegurar que la familia se constituya en un verdadero núcleo central de protección que, en atención al principio de interés superior, pondere "no sólo el requerimiento de medida especiales, sino también las características particulares de la situación en la que se hallan el niño"[59]. Así pues, parece necesario centrar nuestra atención en la primera escuela. Aquella donde se adquieren valores y normas de comportamiento básicos y necesarios para desenvolverse en sociedad: la familia[60].

Bajo estas consideraciones, corresponde señalar cuáles son las obligaciones y el papel que cumple la familia, frente a lo que hemos denominado el "deber de corresponsabilidad", para la protección de datos de los menores. En primer término, señalamos que el concepto de corresponsabilidad se origina del deber que tiene el Estado, la sociedad y la familia, en relación al aseguramiento y respeto de los derechos fundamentales en la comunidad. Como señala la CIDH:

> No hay que perder de vista las limitaciones existentes en diversas materias, como el acceso de los padres al menor. Algunas de estas medidas constituyen un peligro para las relaciones familiares. Debe existir un balance justo entre los intereses del individuo y los de la comunidad, así como entre los del menor y sus padres. La autoridad que se reconoce a la familia no implica que ésta pueda ejercer un control arbitrario sobre el niño, que pudiera acarrear daño para la salud y el desarrollo del menor[61].

[58] Véase, Memorándum de Montevideo, 2009.
[59] Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-17/2002 relativa a la condición jurídica y derechos humanos del niño, solicitada por la Comisión Interamericana de Derechos Humanos.2002.
[60] En todo caso, aquel núcleo fundamental donde deben promoverse derechos y obligaciones recíprocas.
[61] Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-17/2002 relativa a la condición jurídica y derechos humanos del niño, solicitada por la Comisión Interamericana de Derechos Humanos.2002.

En la era digital, la corresponsabilidad u obligaciones que corresponden a la familia es fundamental, dado que Internet y las redes sociales suponen nuevos paradigmas, en donde los menores desarrollan su personalidad e identidad digital, con lo cual, "la privacidad es un derecho de los niños, así como su identidad en línea, que, a medida que crezcan, la irán armando y, por lo tanto, debe ser definida por ellos y no por sus padres"[62]. Desde esta perspectiva, destacamos la relevancia de abrir verdaderos espacios de diálogo, supervisión y control en la familia de tal manera que esta libertad informática pueda encajar con el desarrollo integral de los menores. A tal efecto, "se debe aconsejar a las familias sobre estos temas, ya que los padres pueden no tomar en cuenta que, al utilizar las redes sociales, pueden afectar el bienestar de sus hijos"[63].

Por ejemplo, la Agencia Española de Protección de Datos, en relación a la sobreexposición de datos personales en Internet recomienda, por un lado, reflexionar antes de publicar cualquier tipo de información personal o imágenes, y así también evitar compartir datos considerados como sensibles o especialmente protegidos[64]. Esta práctica denominada *oversharing* presenta mayores riesgos, "cuando la información que se comparte está protagonizada por los menores. Dado que, si bien no cabe duda de la buena intención de los padres al compartir fotografías y vídeos —tiernos, graciosos, llamativos u originales— de sus hijos, la pregunta que debemos hacernos es ¿vulnera esta actitud el derecho del menor a la intimidad, el honor y la propia imagen?[65]. Una pregunta de difícil respuesta. No obstante, subrayamos que "los niños poseen los derechos que corresponden a todos los seres humanos –menores y adultos– y tienen además derechos

[62] Otero, "Sharenting… ¿la vida de los niños debe ser compartida en las redes sociales?", 412.
[63] Ibíd.
[64] Agencia Española de Protección de Datos. Infografía sobre Protección de Datos y Prevención de Delitos. Disponible en https://tinyurl.com/yy2rauon. La AEPD, denomina como "*Oversharing*" a la "sobreexposición de información personal en Internet, en particular en las redes sociales a través de los perfiles de los usuarios".
[65] Laura Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. 23.

especiales derivados de su condición, a los que corresponden deberes específicos de la familia, la sociedad y el Estado"[66].

Al abundar información de menores en entornos digitales, riesgos a los que se exponen no deben pasar desapercibidos, ya que pueden afectar bienes jurídicos especialmente protegidos, relacionados con el desarrollo de su personalidad, integridad, privacidad, la propia imagen y derecho a la identidad digital. Por esta razón, es indispensable "promover la sensibilización y la comprensión de todos los agentes implicados acerca de los riesgos, normas, garantías y derechos relativos a la utilización de las Redes Sociales, haciendo hincapié en que las actividades dirigidas específicamente a los menores de edad"[67]. Así, en la familia, entre los deberes específicos llamados a precautelar la seguridad, bienestar y desarrollo de los menores en la web se destacan, además:

1. La prevención, —sin dejar de lado un enfoque de políticas, normativo y judicial— para enfrentar los aspectos identificados como riesgosos de la Sociedad de la Información y Conocimiento, en especial del Internet y las redes sociales digitales, fundamentalmente por medio de la educación.
2. Proveer información y fortalecer capacidades de los progenitores y personas responsables, sobre los eventuales riesgos a los que se enfrentan las niñas, niños y adolescentes en los ambientes digitales[68].

En este orden de ideas, hemos destacado la importancia de promover una cultura digital para la protección de datos, por medio del deber de corresponsabilidad que tiene la familia. La prevención, basada en la sensibilización y educación, sobre los riegos que suponen compartir información personal de los menores, es esencial, destacándose el papel que cumplen los padres y personas responsables del cuidado de los menores. Por ello, insistimos en que "es sobre todo a través de la educación que [sic] gradualmente se supera la vulnerabilidad de los niños"[69]. Es

[66] Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-17/2002 relativa a la condición jurídica y derechos humanos del niño, solicitada por la Comisión Interamericana de Derechos Humanos.2002.
[67] Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*, 98.
[68] Véase, Memorándum de Montevideo, 2009.
[69] Véase, Corte Interamericana de Derechos Humanos. Opinión consultiva OC-17/2002 relativa a la condición jurídica y derechos humanos del niño, solicitada por la Comisión Interamericana de Derechos Humanos.2002.

esencial que los padres y quienes comparten el vínculo familiar fortalezcan sus capacidades "sobre el impacto de las imágenes subidas a Internet, así como la conveniencia de hacer conscientes tanto a los menores como a los adultos de los derechos y deberes —de unos y de otros— respecto al uso de Internet en general y de las Redes Sociales en particular"[70]. De este modo, cobra especial significación la tutela de los derechos digitales de los menores, por cuanto, solamente, garantizando un equilibrio, entre deberes y derechos en la sociedad de la información, podremos estimar que el tratamiento de la información de los menores cumple con el deber de corresponsabilidad a la que están sujetos el Estado, la sociedad y la familia.

## 4. Derechos de los menores en la Ley Orgánica de Protección de Datos Personales en Ecuador

A partir del desarrollo y expansión de las tecnologías de la información y comunicación, el derecho a la protección datos de los menores ha llegado a significar una de las principales preocupaciones. En este aspecto, el art. 7 del PLODP 2016 consideró que:

> Se asegurará el respeto al derecho a la intimidad de las niñas, niños y adolescentes, por lo que se prohíbe el tratamiento de sus datos personales, salvo aquellos datos que sean de naturaleza pública. Es deber del Estado y de las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan las niñas, niños y adolescentes respecto al tratamiento indebido de sus datos personales; y proveer de conocimiento acerca del uso responsable y seguro por parte de niñas, niños y adolescentes de sus datos personales, su derecho a la intimidad y protección de su información personal y a la de los demás.

En cambio, el art. 40 del PLODP 2019 garantizaba que el tratamiento de datos de los menores se cumpliría bajo los principios de lealtad, transparencia e información. Así, sobre la base de estos principios, dicha propuesta manifestó que en el caso "de productos o servicios digitales utilizados por menores la información será proporcionada a su representante legal" –art. 23 *in fine*–. En todo caso, consideró

[70] Davara Fernández, *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*, 24.

que la información relativa a la niñez y la adolescencia constituían categorías especiales de datos personales –art. 38–. De esta manera, finalmente, la LOPD ha concretado que, primero, los datos de los menores son considerados como una categoría especial –art. 25. b)–; y, segundo, a partir del derecho a la información, atendiendo los principios de lealtad y de transparencia, "en el caso de productos o servicios dirigidos, utilizados o que pudieran ser utilizados por niñas, niños y adolescente la información será proporcionada a su representante legal" –art. 12 *in fine*–. Ahora bien, en el contexto internacional, el RGPD dispone que los menores merecen una protección específica aplicada, particularmente "a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño" –Considerando 38–.

Así también los EPEI reconocen que la niñez y la adolescencia "demandan de garantías adecuadas y suficientes de protección frente a usos indebidos o arbitrarios de su información personal, preservando de esta manera su interés superior, el libre desarrollo de su personalidad, su seguridad y otros valores que son objeto de máxima protección" –Considerando 13–[71]. De la misma manera, el Memorándum de Montevideo formula algunas recomendaciones en la materia, entre las que se destacan a la prevención, sin olvidar la importancia de las políticas públicas, normas y decisiones judiciales. Así, con el objeto de ejercer un mejor control sobre el tratamiento de la información personal de la niñez y la adolescencia, este instrumento también determina que debe protegerse la información personal de los menores "sin que se afecte su dignidad como personas ya que ellos tienen una expectativa razonable de privacidad al compartir su información en ambientes digitales, dado que consideran que se encuentran en un espacio privado".

Es notorio que los menores pueden verse expuestos a mayores riesgos. Por ello, cobra especial importancia que la LOPD en Ecuador asegure en su regulación que

[71] Los EPEI agregan que "en el tratamiento de datos personales concernientes a niñas, niños y adolescentes, los Estados Iberoamericanos privilegiarán la protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral" –art. 8.1–.

los menores tengan una protección respecto a sus derechos digitales. En este orden, tiene que señalarse que, tanto las propuestas de Ley como la LOPD, aprobada en mayo de 2021, han reconocido que el tratamiento de datos de los menores debe respetar el ordenamiento jurídico, estableciendo la necesidad de proveer información y conocimiento, sobre los riesgos y amenazas a los que se enfrentan la niñez y la adolescencia en el mundo virtual. Como señala la Guía legislativa de la OEA, la definición de los datos sensibles debe establecerse en cada legislación o normativa nacional, atendiendo a su entorno cultural y jurídico[72]. En el caso de la Unión Europea, se estima que "los datos sobre menores no tienen el carácter de categorías especiales de datos personales, pero merecen una atención especial. Por ese motivo, el RGPD (…) ha regulado la protección de los menores en lo que respecta al tratamiento de sus datos personales"[73]. Así, como hemos anotado, los EPEI sugieren el mismo modelo de regulación que propone el RGPD.

Respecto a las normas sobre la garantía de derechos digitales, un ejemplo significa la LOPDGDD en España, puesto que, reconoce la protección de los menores en Internet. Así, se desprende en su objeto al garantizar "los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución" –art. 1. b)–[74]. En este caso, a la luz de las propuestas que hemos estudiado en Ecuador, únicamente, el PLODP 2019 hizo referencia en su objeto a que la Ley

[72] La Guía legislativa de la OEA, sobre la tipología de datos sensibles anota que: "se reconoce que la sensibilidad de los datos personales puede variar según la cultura y cambiar con el tiempo y que los riesgos de ocasionar daños reales a una persona como consecuencia de la divulgación de datos podrían ser insignificantes en una situación en particular, pero podrían poner en peligro la vida en otra".

[73] Antonio Troncoso, "Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales", *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada*, Nro. 49 (2018), 187-266.

[74] Desde esta perspectiva, asumimos que "el reconocimiento constitucional o europeo, legal o constitucional, del derecho fundamental a la protección de datos no agota la necesidad de establecer un nuevo marco de protección de los ciudadanos en la era digital. Esto es, resulta ineludible la necesidad de reconocer nuevos derechos digitales bien en el ámbito legal como constitucional (…) La tecnología constituye una realidad que nos envuelve y que condiciona nuestros comportamientos más cotidianos. Internet es una realidad omnipresente. La transformación digital de nuestra sociedad es una realidad en constante desarrollo. Países como Italia o Francia han aprobado una Declaración de Derechos en Internet o una legislación de impulso digital reforzando los derechos digitales de la ciudadanía". Cfr. Rallo Lombarte, "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)", 665-666.

regularía “el ejercicio del derecho a la protección de datos, la autodeterminación informativa y demás derechos digitales” –art. 1–. Sin embargo, en la LOPD, el legislador ha restringido que el objeto y finalidad de la Ley se concentra, únicamente, en garantizar el ejercicio del derecho a la protección de datos personales –art. 1–.

Por otra parte, destacamos que, sobre los derechos en la era digital, la LOPDGDD señala que “los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet” –art. 79–[75]. Por ejemplo, el derecho a la neutralidad de Internet precisa que “los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos” –art. 80–. Además, el art. 81 garantiza el derecho de acceso universal a Internet [76], y el derecho a la seguridad digital, mediante el cual, “los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos” –art. 82–. En este ámbito, el art. 83 de la LOPDGDD reconoce el derecho a la educación digital, por el cual:

> 1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.
>
> Las Administraciones educativas deberán incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital a la que se refiere el apartado anterior, así como

[75] La LOPDGDD agrega que “los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación”.

[76] Por ejemplo, dispone que “1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica; 2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población; 3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral; 4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores; 5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales; 6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales”.

> los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.
>
> 2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.
>
> 3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.
>
> 4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

Además, en relación a la protección de datos de los menores en Internet, el art. 92 de la LOPDGDD determina que:

> Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.
>
> Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales.

Si bien, no existieron apartados específicos en las propuestas de Ecuador respecto a la garantía de derechos digitales, el art. 35 del PLODP 2019 ha materializado en la LOPD el reconocimiento del derecho a la educación digital –art. 23–, como parte de las libertades que corresponde asegurar a los titulares de los datos personales, precisando que:

> Las personas tienen derecho al acceso y disponibilidad del conocimiento, aprendizaje, preparación, estudio, formación, capacitación, enseñanza e instrucción relacionados con el uso y manejo adecuado, sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación, en estricto apego a la dignidad e integridad humana, los derechos fundamentales y libertades individuales con especial énfasis en la intimidad, la vida privada, autodeterminación informativa, identidad y reputación en línea, ciudadanía digital y el derecho a la protección de datos, así como promover una cultura sensibilizada en el derecho de protección de datos personales.
>
> El derecho a la educación digital tendrá un carácter inclusivo sobre todo en lo que respecta a las personas con necesidades educativas especiales.
>
> El sistema de educación nacional, incluyendo el sistema de educación superior, garantizará la educación digital no solo a favor de los estudiantes de todos los niveles sino también de los docentes, debiendo incluir dicha temática en su proceso de formación.

Siguiendo el esquema de protección de la LOPDGDD, la LOPD propone una regulación semejante al garantizar el derecho a la educación digital, frente a las

amenazas y riesgos que supone el uso de tecnologías de la información y comunicación. En este contexto, si bien, en su objeto no se propone regular y garantizar la protección de los derechos digitales, que se derivan del tratamiento y flujo de datos personales, parece necesario extender en la normativa de protección de datos otras prescripciones que desarrollen la protección y tutela integral de las personas en Internet. Por ejemplo, harían falta regulaciones relacionadas con el derecho de rectificación en Internet; derecho a la actualización de informaciones en medios de comunicación digitales; derecho al testamento digital. Además, en el ámbito laboral, regulaciones sobre el derecho a la intimidad y uso de dispositivos digitales; derecho a la desconexión digital; derecho a la intimidad, frente al uso de dispositivos de videovigilancia y de grabación de sonidos; derecho a la intimidad, ante la utilización de sistemas de geolocalización. En este marco, además es imprescindible extender la protección de datos de los menores en Internet[77], lo cual, en todo caso, podría materializarse en la normativa sectorial, atendiendo el art. 11 de la LOPD.

Como hemos advertido, la protección de los derechos a la intimidad y privacidad concretan, en muchas ocasiones, la tutela del derecho a la protección de datos personales[78], por cuanto el derecho a la privacidad "alcanza también a los dispositivos informáticos que utilizamos y que forman parte ya de nuestra propia vida, que contiene información que nos identifica y que puede dar una imagen de nuestra personalidad. Lo que supone para tal derecho, para la protección de datos,

[77] En todo caso, sobre la protección y garantía de los derechos de los menores en Internet, recordemos que el Código de la Niñez y la Adolescencia, por ejemplo, prohíbe "la circulación de publicaciones, videos y grabaciones dirigidos y destinados a la niñez y adolescencia, que contengan imágenes, textos o mensajes inadecuados para su desarrollo; y cualquier forma de acceso de niños, niñas y adolescentes a estos medios" –art. 46.1–. Por tanto, tan inadecuados pueden resultar los mensajes dedicados a manipular o difundir fotografías sin el consentimiento del titular de los datos personales (*Morphing*), como también discriminar, hostigar, humillar y acosar a otra persona, en razón de sus creencias religiosas, ideología política, convicciones morales o condiciones de salud personal (*Ciberbullying o Grooming*). Así, es fundamental que el uso de tecnologías de la información y comunicación se equilibren con el respeto del derecho a la protección de datos, particularmente, de los menores".

[78] Como destaca el Memorándum de Montevideo, "el derecho a la vida privada es un valor que toda sociedad democrática debe respetar. Por tanto, para asegurar la autonomía de los individuos, decidir los alcances de su vida privada, debe limitarse el poder tanto del Estado como de organizaciones privadas, de cometer intromisiones ilegales o arbitrarias, en dicha esfera personal".

un desarrollo espectacular[79]. Sirva de ejemplo, las intromisiones en la intimidad como resultado del "*shareting*" (sobre exposición en redes sociales, especialmente, de niños y niñas, como resultado de compartir perfiles e imágenes por parte de los padres); y también aquellas intromisiones sobre la correspondencia y comunicaciones, como consecuencia del "*sexting*" (circulación de mensajes de texto, a través de imágenes y videos con contenido sexual). Todo ello, deriva en actitudes que afectan a la propia información personal que se protege por medio del derecho a la protección de datos; y que, en todo caso, representan, "también en muchas ocasiones una concretización del derecho a la intimidad en los tratamientos de datos personales, un derecho más específico dentro del más general derecho de privacidad personal"[80].

La aparición de nuevas tecnologías, como Internet y redes sociales, simbolizan un cambio de paradigma en la protección de los datos, de la intimidad y la privacidad de la personas[81]. Las redes sociales "son grandes fuentes de información no sólo de sus miembros sino sobre las personas que éstas conocen o han contactado alguna vez y suponen tratamientos masivos de datos personales, lo que representa un riesgo para la privacidad de las personas"[82]. Por esta razón, advertimos que la aparición de los "nativos digitales" plantea nuevas problemáticas y tensiones, entre el uso de las tecnologías y la protección de los derechos y libertades[83].

Entre otras medidas, un adecuado marco jurídico de protección y la ejecución de verdaderas políticas de concienciación, pueden consolidar las bases de un entorno equilibrado en la defensa de los derechos de la niñez y la adolescencia. El respeto

[79] Lucas Murillo de la Cueva y Piñar Mañas, El *derecho a la autodeterminación informativa*, 101.
[80] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 69**.**
[81] Por ello, es importante priorizar los mecanismos de protección de la información de carácter personal, frente a los avances experimentados en la sociedad de la información. Así, los EPEI señalan la necesidad de ser conscientes "acerca de los riesgos potenciales que pueden derivarse en la esfera de las personas físicas con motivo del tratamiento de sus datos personales a gran escala efectuado por parte de organismos públicos y privados y, en particular, teniendo en cuenta la especial vulnerabilidad de las niñas, niños y adolescentes" –Considerando 13–.
[82] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1693**.**
[83] El concepto de nativos digitales nació con Marc Prensky, para denominar a todos lo que "han nacido y se han formado utilizando la particular "lengua digital" de juegos por ordenador, video e Internet". Cfr. Marc Prensky, "Nativos e Inmigrantes Digitales", *Cuadernos SEK 2.0 – Institución Educativa SEK,* Depósito legal: M-24433 (2010): 1-20.

del derecho a la protección de datos conlleva la tutela de otras libertades y bienes jurídicos derivados, por cuanto en la era digital, la falta de respeto a la intimidad y privacidad de la información personal –por medio de tipologías como el *grooming, shareting, sexting, morphing y ciberbullying*, etc.– pueden lesionar, gravemente, a la dignidad, honra, imagen y derechos relacionados con el libre desarrollo de la personalidad de los menores.

## 5. La necesidad de políticas públicas y programas para la promoción de los derechos y obligaciones relativas al derecho fundamental a la protección de datos personales, en especial de los niños, niñas y adolescentes

Como plantea el Memorándum de Montevideo, es imprescindible desarrollar políticas públicas tendentes a garantizar en el entorno digital la protección de datos personales y el derecho a la intimidad de los menores[84]. Considerando este instrumento, en esta parte final, abordaremos el alcance de los programas y políticas, que requieren en la práctica este derecho fundamental, especialmente, en la niñez y la adolescencia. Así también, a partir de la experiencia de modelos jurídicos que han recibido reconocimiento internacional dentro de la región, intentaremos proponer un modelo de protección, el cual asegure las medidas especiales, en entornos digitales, ya que "garantizar la protección de datos personales y la privacidad son clave para generar la confianza necesaria en la innovación"[85], tanto en el ámbito público como privado.

A partir del ejercicio del desarrollo integral de los menores, por disposición constitucional, las políticas públicas intersectoriales nacionales y locales permitirán

[84] Al respecto, este instrumento señala que "los niños, niñas y adolescentes tienen cada vez mayor acceso a los distintos sistemas de comunicación, que les permiten obtener todos los beneficios que ellos representan, pero esta situación también ha llevado al límite el balance entre el ejercicio de los derechos fundamentales y los riesgos —para la vida privada, el honor, buen nombre, y la intimidad, entre otros— que, así como los abusos de los cuales pueden ser víctimas —como discriminación, explotación sexual, pornografía, entre otros— pueden tener un impacto negativo en su desarrollo integral y vida adulta".

[85] Recio Gayo, *Protección de datos personales e Innovación: ¿(In) compatibles?,*17.

“la satisfacción de sus necesidades sociales, afectivo-emocionales y culturales” –art. 44–. En este ámbito, además, el art. 46.7 de la Constitución precisa que el Estado ecuatoriano deberá adoptar, entre otras medidas:

> Protección frente a la influencia de programas o mensajes, difundidos a través de cualquier medio, que promuevan la violencia, o la discriminación racial o de género. Las políticas públicas de comunicación priorizarán su educación y el respeto a sus derechos de imagen, integridad y los demás específicos de su edad. Se establecerán limitaciones y sanciones para hacer efectivos estos derechos.

La necesidad de crear espacios para la promoción de los derechos de la niñez y la adolescencia, sobre todo, para aquellos derechos vinculados con el uso de las tecnologías de la información y comunicación, es una necesidad imperiosa[86]. Un ejemplo, encaja, perfectamente, en la protección de la privacidad e intimidad, que resulta de la difusión e intercambio de información, por medio de las redes sociales, por cuanto:

> Las redes sociales, basadas en que los usuarios comparten información a veces muy sensible, suponen un reto a la privacidad personal e implican un cambio de paradigma. El propio concepto de red social conlleva una cierta renuncia de los usuarios a su privacidad. Las personas ponen en común aficiones, gustos y vivencias con la finalidad de facilitar el acceso a esta información por una red de contactos que incluye una mayoría de personas a las cuales no conocen[87].

Por todo esto, impera que en la sociedad de la información se garantice la protección de las personas, frente a los riesgos que se desprenden del uso de las tecnologías. Más aún, si se trata de un grupo de atención prioritaria, como es el caso de la niñez y la adolescencia, debe atenderse el principio de interés superior, no solamente por medio de su reconocimiento normativo y jurisprudencial sino también, a través de su garantía en la práctica. En este punto, el Memorándum de Montevideo recomienda “establecer sistemas de información para que, aquellas niñas, niños y adolescentes que tengan alguna preocupación por los contenidos en Internet o las redes sociales digitales, puedan tener asesoría y apoyo rápido”[88]. Así,

[86] Como precisa la Guía legislativa de la OEA, “cada Estado Miembro debe determinar cuál es la mejor manera de implementar estos principios en su ordenamiento jurídico interno. Sea por medio de Leyes, normas u otros mecanismos”.
[87] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1693**.**
[88] Por ejemplo, el Memorándum sugiere “generar medidas como ayuda y denuncia en línea, números gratuitos telefónicos, centros de atención, etc.”.

la implementación de sistemas de información, como mecanismos de concienciación, mediante políticas públicas, constituye una medida idónea para difundir las libertades informáticas, que forman parte del desarrollo y ejercicio del derecho a la protección de datos[89].

En el caso de Ecuador, desde la aprobación de la LOPD, queda analizar el desarrollo del derecho a la protección de datos personales por medio de políticas públicas. Pero, ¿qué son las políticas públicas? o ¿qué características deben cumplir éstas en la práctica para concretar el desarrollo de este derecho fundamental? En sentido general, las políticas públicas existen siempre y cuando "instituciones estatales asuman total o parcialmente la tareas de alcanzar objetivos estimados como deseables o necesarios, por medio de un proceso destinado a cambiar un estado de las cosas percibido como problemático"[90]. Este concepto supone la idea de un cambio, a partir de la identificación de un problema que requiere atención y regulación, desde la instancia gubernamental. En todo caso, entendemos que éstas emergen "de una construcción social y de una construcción de un objeto de investigación"[91], y que se orientan a definir el quehacer del Estado, frente a un determinado problema.

No se puede desconocer que, en el caso de Ecuador, existe implicación del gobierno para la protección de los derechos relativos a los menores. La creación de instituciones –como el Consejo Nacional de la Niñez y la Adolescencia (CNNA), Consejos Cantonales y Juntas Cantonales de Protección de Derechos– se orientan a instituir un Sistema Nacional Descentralizado de Protección Integral de la Niñez y la Adolescencia[92]. No obstante, en materia de protección de datos de los menores,

---

[89] Como advierte Antonio Troncoso, son tres los aspectos que deben considerarse para la protección de los datos personales en redes sociales. A saber: la legislación, la autorregulación y la concienciación de los usuarios. Cfr. Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1694.

[90] André-Noel Roth Deubel, "Políticas Públicas: Formulación, Implementación y Evaluación", *Ediciones Aurora,* (2002): 1-134.

[91] Ibíd. Según Roth Deubel, la existencia de políticas públicas se caracteriza por la identificación de cuatro elementos centrales, a saber: "implicación del gobierno, percepción de problemas, definiciones de objetivos y proceso".

[92] Véase el art. 192 del Código de la Niñez y la Adolescencia. Así también puede considerarse los ejes estratégicos 1 y 2 del Ministerio de Inclusión Económica y Social que, en la materia consideran:

poco o nada se ha hecho. Por lo que, como menciona el Memorándum de Montevideo, es necesario promover en éstas un compromiso "para asegurar su participación en la protección y en las campañas de alerta sobre las potencialidades y los riesgos de Internet y las redes sociales digitales". En Ecuador, las políticas públicas derivadas de la protección de datos son un paradigma que aún se encuentra en construcción. Como hemos apuntado, anteriormente, tanto las propuestas legislativas de 2016 y 2019 como ahora la LOPD pretenden construir un sistema de protección y tutela para el derecho a la protección de datos. No obstante, corresponde señalar que este sistema también se construye, a través de políticas públicas, como un medio de desarrollo de los derechos reconocidos en la Constitución. Desde ya, existen determinadas cuestiones que –a la luz de experiencias y modelos internacionales–; los sectores públicos deben asumir, frente al planteamiento de políticas adecuadas para el aseguramiento del derecho a la protección de datos, especialmente, en el caso de los menores.

En este aspecto, el Memorándum de Montevideo recomienda que:

> La protección de los datos personales requiere del desarrollo de una normativa nacional, aplicable al sector público y privado, que contenga los derechos y principios básicos, reconocidos internacionalmente, y los mecanismos para la aplicación efectiva de la misma. Los Estados deberán tomar en especial consideración, en la creación y en el desarrollo de dichas normativas, a las niñas, niños y adolescentes.

Puede señalarse que el Memorándum de Montevideo, la Guía Legislativa de la OEA, los EPEI, la normativa europea y la aprobación de la LOPD deberían inspirar las bases para una protección adecuada, no solamente para desarrollar en la normativa sectorial el derecho a la protección de los datos sino también para la formulación de políticas que ayuden en el desarrollo efectivo de los derechos

---

Eje Nro.1: Protección Especial.- Garantizar políticas y regulaciones para la protección especial, con la finalidad de promover, proteger y restituir los derechos de las y los ciudadanos en todo su ciclo de vida, con énfasis en niños, niñas, adolescentes adultos mayores personas con discapacidad, en corresponsabilidad con la comunidad que aseguren el ejercicio, garantía y exigibilidad de los derechos; y Eje Nro.2: Desarrollo Integral.- Garantizar la gestión estratégica en la formulación, aplicación e implementación de las políticas, programas, normas e instrumentación que permitan fomentar y garantizar los derechos de niños y niñas, adolescentes, jóvenes, adultos mayores y personas con discapacidad en el Ecuador para el ejercicio pleno de su ciudadanía en libertad e igualdad de oportunidades en el marco del Buen Vivir.

digitales, que corresponden a las personas y, en particular, a la niñez y la adolescencia[93]. A pesar de la existencia de entidades gubernamentales dedicadas a la protección integral de la niñez y la adolescencia, la situación se encuentra en un estado de penumbra[94]. En los últimos años, esta realidad no ha cambiado. Si hacemos referencia a programas para el proceso de aplicación de políticas vinculadas con la protección de datos; el escenario se encuentra desamparado.

Hoy en día, existe más acercamiento de los menores a medios relacionados con el mundo tecnológico, como Internet y redes sociales. Por ello, desde las grandes habilidades digitales, que demuestran la niñez y la adolescencia en el campo de la

[93] En todo caso, en la materia, una interesante propuesta significó el Proyecto de Ley que regularía los "actos de odio y discriminación en redes sociales e Internet". En su exposición de motivos señala que como resultado del avance y desarrollo de las tecnologías de la información "el intercambio de la información podría afectar a las personas, existiendo la posibilidad de llegar a ser víctimas de prácticas ilícitas que se realizan en la red, pudiendo ser estafadas, o sufrir la sustracción de su información personal, entre otras infracciones potenciales en la red". Considerando que este proyecto se afianza en el respecto y protección de los derechos y ciudadanos en la red y plataformas de Internet, se expone que, además, "se calcula que, en la República del Ecuador, existen alrededor de once millones de usuarios de la red social Facebook, es decir se encuentran inscritas igual número de cuentas. Las redes sociales restantes reportan un importante número de registros: i) Instagram con un millón y medio; ii) Linkedln alcanza el millón ciento setenta mil; y iii) Twitter setecientos mil".

[94] Conviene señalar que, Ecuador en 2011 –dentro del décimo informe ante el Secretario General de la OEA sobre las medidas emprendidas por los Estados miembros para prevenir y erradicar la explotación sexual comercial de niñas, niños y adolescentes en las Américas (ESCNNA)– informó dos cuestiones que, en este punto, son importantes mencionar. Primero, que no contaba con programas o políticas específicas "dirigidas a prevenir el uso no seguro e irresponsable de las TIC"; y segundo, que el Consejo Nacional de la Niñez y Adolescencia ha encaminado "un proyecto de monitoreo de eventos y contenidos de Internet referidos a la pornografía infantil, la venta de niños, niñas y adolescentes". Para ese entonces, este informe estimaba que el número de usuarios de Internet en América había crecido en "un 253.9% en el período 2000-2009. En diciembre del año 2009 se estimaban 446.483.050 usuarios de la red, lo que representaba un 24.8% del total de usuarios del mundo (1.802.330.457) y un 48% de la población del continente". Asimismo, este informe agregaba que existía "una fuerte tendencia al crecimiento de la cantidad de usuarios en América Latina y el Caribe"; y en lo relativo a las tipologías, que se producen por la inobservancia de las reglas que protegen el tratamiento de la información personal, señalaba que: "conforme se van desarrollando herramientas y plataformas que habilitan la autogeneración de contenido y el libre intercambio de información –que tanto promueve el derecho a la libre expresión de los niños–, también, en paralelo, se abre un escenario en el que los delincuentes sexuales tienen más posibilidades de compartir imágenes y tener contacto con niños, de una manera antes desconocida. Por este motivo, la comunidad internacional ha expresado su preocupación al detectar las distintas maneras en las que niños, niñas y adolescentes pueden estar siendo explotados por medio de las TIC". Cfr. El X Informe al Secretario General de la OEA sobre las medidas emprendidas por los Estados Miembros para prevenir y erradicar la Explotación Sexual Comercial de niñas, niños y adolescentes en las Américas (ESCNNA). Disponible en: http://www.iin.oea.org/pdf-iin/Explotacion-sexual-comercial-version-digital.pdf.

comunicación digital. Es indispensable establecer las bases para el desarrollo de una cultura digital, que se oriente a concienciar en la sociedad y la familia sobre el valor que representa cuidar los datos personales. Particularmente, es esencial que los riesgos y amenazas que representan las Tics, frente al tratamiento de la información personal, formen parte de la agenda política del Estado ecuatoriano[95].

Para este fin, por ejemplo, el Memorándum de Montevideo sugiere:

> Impulsar la generación de conocimiento especializado con el fin de elaborar políticas públicas adecuadas. En especial, en lo que refiere a los comportamientos en línea de niñas, niños y adolescentes, se sugiere investigar acerca de los roles que estos juegan en la recepción, producción, almacenamiento y reproducción de contenidos ilegales, las medidas de protección que ellos mismos desarrollan, las motivaciones individuales y colectivas de dichos comportamientos, así como los peligros reales a los que se enfrentan en la Sociedad de la Información y el Conocimiento.

De este modo, el planteamiento es "concienciar a los usuarios, especialmente a los jóvenes, acerca de la información que publican en estas redes sociales, para que valoren la importancia de su intimidad y la protección de sus datos personales"[96]. En el ámbito internacional, un buen ejemplo de estas buenas prácticas, sobre cultura digital, representa la actividad que desarrollan las autoridades de control, que han recibido reconocimiento internacional. Como hemos señalado en otro momento, dentro de la Comunidad Andina, Argentina y Uruguay constituyen relevantes modelos que deben ser analizados, como referentes de desarrollo, para el fin de materializar un modelo de cultura digital[97].

---

[95] En todo caso, hay que destacar la "Política pública por una internet segura para niñas, niños y adolescentes", aprobada por el Estado ecuatoriano en septiembre de 2020. Ésta tiene por objeto establecer una política de uso sano, seguro y constructivo de la internet, para niños, niñas y adolescentes y, en suma, "potenciar las oportunidades y habilidades que ofrecen las tecnologías digitales en su vida y su desarrollo, y así, promover el aprovechamiento de los usos y beneficios de las TIC en un marco de derechos (digitales), dignidad e integridad física, psicológica, emocional y sexual. Se trata de una política destinada a promover conductas protectoras o preventivas de factores de riesgos que pueden poner en peligro la integridad y dignidad de niñas, niños y adolescentes ante el acceso y uso de internet; y cuando tales vulneraciones han sucedido, promover protocolos adecuados de atención para la protección, atención y reparación". Disponible en: https://www.igualdad.gob.ec/wp-content/uploads/downloads/2020/09/pol%C3%ADtica_publica_internet_segura.pdf

[96] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1711**.**

[97] La Comunidad Andina, actualmente, está conformada por cuatro países miembros: Bolivia, Colombia, Ecuador y Perú; por cinco países asociados: Chile, Argentina, Brasil, Paraguay y Uruguay; y por un país observador: España.

En el caso de Argentina, la Dirección Nacional de Protección de Datos Personales (DNPDP) fue reconocida en 2014 por el “Berkman Klein Center for Internet & Society” de la Universidad de Harvard, en virtud, del programa nacional "Con Vos en la Web", considerándolo como una propuesta de política pública exitosa en la región. En la práctica, esta autoridad de control ha establecido medidas tendentes a asegurar el derecho a la protección de datos, mediante la creación de un campus virtual, de talleres y capacitaciones; difusión de materiales, como guías para el cuidado de los datos personales de los jóvenes y manuales, sobre la Ley 25.326 en su versión para menores; y videos tutoriales, para padres en la web.

En lo que corresponde a Uruguay, la Unidad Reguladora y de Control de Datos Personales (URCDP) ha consolidado la propuesta educativa “Tus datos valen. Cuídalos”; la cual introduce temas relacionados con la protección de datos personales, por medio, de una mirada integral en la que confluyen niños, padres y docentes. Así, la URCDP propone, tres líneas de acción, encaminadas a sensibilizar y capacitar a la ciudadanía en materia de protección de datos, mediante la formación técnica, concursos para niños e inserción en programas de formación docente.

Finalmente, destacamos la actividad que viene desarrollando la Agencia Española de Protección de Datos (AEPD), por cuanto colabora con el programa “Tú decides en Internet”. Así, como se señala en su página web, su contenido “está elaborado para que los niños y adolescentes puedan obtener información y consejos sobre cómo utilizar sus datos de carácter personal y de otras personas especialmente en el mundo de Internet, a través de una serie de materiales como guías, vídeos, cómic, test y juegos, presentados de manera visual y atractiva”.

Todo este escenario conlleva realizar un análisis, no solo de la importancia de una normativa en la materia sino también de la necesidad de posibilitar modelos conducentes a afianzar una cultura digital del derecho a la protección de datos, en particular, de la niñez y la adolescencia. En efecto, estimar mecanismos de control y prevención, plasmados en un modelo de cultura digital, respecto a los riesgos que representan sufrir amenazas, intimidación, extorsión y discriminación; es una tarea que debe afianzarse en los modelos jurídicos de los Estados. Considerando que, “la

privacidad es un derecho de los niños, así como su identidad en línea, que, a medida que crezcan, la irán armando y, por lo tanto, debe ser definida por ellos y no por sus padres"[98]; la educación digital se plantea como una garantía que puede estar orientada a que los menores hagan conciencia de la protección de sus derechos en Internet y redes sociales. En este orden, son dos los presupuestos, que requieren redefinirse para concretar un modelo de cultura digital de protección de datos en entornos digitales, a partir de políticas públicas. Tanto el contenido esencial de este derecho, como los efectos que las Tics proponen en los sistemas jurídicos, para garantizar su tutela efectiva; son cuestiones que se deben repensar en todo momento.

De hecho, además, hay que tomar en cuenta que "la mayoría de los niños, y muchos progenitores, tienen una conciencia muy limitada, si es que tienen alguna, de la cantidad de datos personales que están proyectando en Internet, y mucho menos sobre cómo podrían ser utilizados algún día"[99]. De este modo, el contenido del derecho a la protección de datos en entornos digitales adquiere especial connotación. Producto de los avances tecnológicos y de los presupuestos que exige este derecho fundamental, es esencial crear escenarios de confianza. Por esta razón, advertimos que, "buena parte del problema sigue estando en la necesidad de restaurar la confianza perdida y encontrar un equilibrio que permita que la innovación pueda avanzar sin frenos indebidos, respetando como garantía la protección de datos personales y la privacidad"[100].

El mundo de las tecnologías exige un cambio de paradigma en la protección de datos en entornos digitales. Abordar el fenómeno tecnológico, frente al tratamiento de la información, requiere analizar las condiciones necesarias que deben desarrollarse para garantizar este derecho fundamental. Por estas razones, la articulación de un modelo de garantía en entornos digitales, por medio de políticas públicas es indispensable. En el contexto de la Comunidad Andina, las bases para

[98] Otero, "Sharenting… ¿la vida de los niños debe ser compartida en las redes sociales?", 412.
[99] Cfr. Unicef (Fondo de las Naciones Unidas para la Infancia), "*El Estado Mundial de la Infancia 2017: Niños en un mundo digital*".
[100] Recio Gayo, *Protección de datos personales e Innovación: ¿(In) compatibles?,* 43.

esta teoría se encuentran desarrolladas, principalmente, en dos instrumentos regionales, que son el Memorándum de Montevideo y los EPEI.

El Memorándum de Montevideo, por ejemplo, recomienda desarrollar procesos de prevención sobre aquellas prácticas digitales, que resulten negativas y afecten el derecho a la protección de datos. Así, como una política de prevención sugiere que:

1. El Estado y entidades educativas provean de información y fortalezcan capacidades de los progenitores y personas responsables, sobre los riesgos a los que se enfrentan las niñas, niños y adolescentes en ambientes digitales.
2. Se transmita a las niñas, niños y adolescentes que Internet no es un espacio sin normas, impune o sin responsabilidades.
3. Se eduque en el uso responsable y seguro de Internet y las redes sociales digitales, en particular sobre: participación anónima; respeto a la vida privada, intimidad y buen nombre de terceras personas; distribución de contenidos que puedan afectar el tratamiento de datos sensibles, como salud, etnia, orientación sexual y política, que puedan llevar a discriminación y acoso en redes sociales; políticas de privacidad, seguridad y alertas; estrategias informativas y formativas sobre los riesgos del uso de Internet y redes sociales, entre otros.
4. Se incluya en los planes de estudios, en todo el currículo educativo, información básica sobre la importancia de la vida privada y de la protección de los datos personales.

Asimismo, según los EPEI, los Estados Iberoamericanos deben promover en la formación académica de los menores, “el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades” –art. 8.2–.

Por último, en el contexto de la Unión Europea, el RGPD se presenta como un instrumento comunitario que exige adecuar la normativa de protección de datos, conforme a los avances que plantea el desarrollo tecnológico. Además, de los

considerandos y preceptos que han sido anotados, anteriormente, se destacan las siguientes disposiciones:

1. Como un mecanismo de prevención, en aquellos casos en que el tratamiento de la información personal suponga un alto riesgo para los derechos y libertades de las personas físicas; corresponde al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo y garantizar la protección de los datos personales.
2. En lo que corresponde a las autoridades de control, entre las actividades de sensibilización del público, deben incluirse medidas en particular al contexto educativo. Así también fomentar la sensibilización del público acerca de los riesgos, las normas, las garantías y los derechos en relación con el tratamiento de datos personales.

Bajos estas consideraciones, si bien, el Estado y la sociedad deben aplicar medidas destinadas a tutelar los derechos de la niñez y la adolescencia, será significativa la función que cumpla la familia. En la sociedad de la información, este triple deber "puede ayudar a las personas, a las comunidades y a los pueblos a alcanzar su pleno potencial, promover el desarrollo sostenible y mejorar la calidad de vida en general"[101]. En este marco, considerando la situación actual en Ecuador, es urgente viabilizar políticas y programas, que permitan concretar prácticas de vigilancia y monitoreo del derecho a la protección de datos, tanto en el ámbito público como privado. Para ello, los instrumentos internacionales, para la protección de datos personales y experiencias desarrolladas en los países de la Comunidad Andina, deben significar los modelos idóneos para formular políticas públicas para su defensa, tutela y aseguramiento, particularmente, en la niñez y la adolescencia.

[101] Cfr. Guía Legislativa de la OEA.

# CAPÍTULO VIII: LAS AUTORIDADES DE CONTROL Y SUPERVISIÓN, FRENTE A LA TUTELA DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES

## 1. Introducción

El derecho a la protección de datos exige de los Estados la adopción de presupuestos necesarios, que aseguren una estructura jurídica integral orientada a brindar a los ciudadanos seguridad jurídica, con relación al tratamiento de su información. Sobre todo, garantizar, institucionalmente, la vigilancia, tutela y el respeto de los derechos que se derivan de la protección de datos. Así, "el reconocimiento de un derecho fundamental exige de los poderes públicos una actividad administrativa de promoción y garantía que se desarrolla mediante tratamiento de datos personales"[1]. Dentro de la actividad de promoción "se encontrarían las funciones que desarrolla la autoridad de control para impulsar los mecanismos voluntarios de autorregulación que favorecen la efectividad del derecho fundamental a la protección de datos personales"[2]. En este sentido, la actividad que desarrollan las autoridades de protección de datos personales favorece en la implementación de mecanismos de protección voluntarios, que flexibilizan el cumplimiento de la legislación de protección de datos.

Existen dos vías que permitirían asegurar la tutela efectiva de este derecho fundamental. La primera relacionada con la vía jurisdiccional que puede entablarse, ante el sistema de administración de justicia ordinaria[3]. Y la segunda, vinculada con

[1] Antonio Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, (Valencia: Tirant lo Blanch, 2010), 33.

[2] Antonio Troncoso, "Autoridades de Control Independientes", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, (Madrid, Reus, 2016), 461-512.

[3] Por ejemplo, en el ámbito de la Unión Europea, la doctrina advierte que "con carácter general, y al margen de las diferencias típicas de los correspondientes ordenamientos jurídicos, ante una violación del derecho a la protección de datos personales su titular puede acudir a las siguientes vías: la vía judicial ordinaria, los Tribunales Constitucionales, el Defensor del Pueblo, el recurso ante el TEDH, y el recurso ante el TJCE. Con la elevación de la Carta de Derechos Fundamentales de la Unión Europea al rango de Derecho originario, tal y como prevé el Tratado de Lisboa, los derechos

una vía no jurisdiccional que pretende, por medio de una autoridad administrativa, ejercer de manera independiente la tutela, vigilancia y el control del derecho a la protección de datos.

Las autoridades de protección de datos tienen especiales particularidades, en cuanto a su organización interna y facultades no jurisdiccionales, que se les confiere por Ley para el ejercicio de sus funciones. Este ejercicio debe abarcar suficientes garantías, que aseguren su independencia, tanto funcional como política, a la hora de supervisar y aplicar la normativa de protección de datos. Al respecto, aclaramos que, el principio de control independiente ejercido por las autoridades de protección de datos es esencial, por cuanto "faltando esa autoridad, no es posible en ningún caso considerar aceptable el marco jurídico regulador del derecho"[4]. En este orden, considerar una autoridad de control en la legislación de protección de datos "resulta coherente con la administrativización de unas relaciones jurídicas, y sirve para proteger a la parte más débil, considerando que el Derecho privado es insuficiente y el Derecho penal excesivo para esta finalidad"[5]. Por ello, insistimos en que su actividad es sustancial en la previsión de mecanismos preventivos para la protección de la información personal, a partir de la concienciación de los derechos que poseen los ciudadanos, en relación al tratamiento de sus datos.

En esta dirección, la protección de este derecho, frente al desarrollo de las tecnologías de la información y comunicación, exige "que las autoridades de control realicen una evaluación de los riesgos y de las garantías necesarias para la protección de datos personales y que va dirigida tanto a responsables y encargados de tratamiento como a ciudadanos"[6]. Si bien, compartimos información personal, sin tomar en cuenta los efectos y riesgos que esto supone, "en todos los casos,

reconocidos en ésta —entre ellos el de la protección de datos personales— se podrán invocar directamente ante el TJCE". Cfr. Mónica Arenas Ramiro, "La protección de datos personales en los países de la Unión Europea", *Revista Jurídica de Castilla y León*, Nro. 16 (2008):113-168.

**4** Pablo Lucas Murillo de la Cueva y José Luis Piñar, El *derecho a la autodeterminación informativa* (Madrid-México: Fontamara S.A, 2011), 104.

**5** Xavier Muroi Bas, "La Agencia de Protección de Datos", *Revista Administración Pública*, Nro. 147 (1998): 381-421.

6 Antonio Troncoso, "Autoridades de Control Independientes", 503.

esperamos que las personas o colectivos que tienen conocimiento de ellos los traten con cuidado, con lealtad y con respeto, con objeto de evitar cualquier tipo de discriminación, marginación o desigualdad por razón de este conocimiento"[7].

En la práctica, esto puede resultar paradójico. Sería, así como esperar que otros respeten nuestros derechos sin que, desde el ámbito individual se haga, absolutamente, nada. Por ello, precisamos que la protección de datos es "un elemento esencial y objetivo que afecta al conjunto de la sociedad y concierne a la calidad de una democracia que demanda ciudadanos libres y con capacidad de decisión"[8]. Precisamente, las actividades que desarrollan las autoridades de control se destinan a supervisar en la comunidad el respeto de todas las libertades, particularmente, el derecho a la protección de datos personales. En definitiva, promover y concienciar las obligaciones que corresponden sobre el tratamiento de la información personal. En todo caso, subrayamos que, además, la autorregulación constituye "una respuesta ágil cuando falte una regulación jurídica en el ámbito nacional o internacional, ante situaciones de gran complejidad técnica o ante la imposibilidad de llegar a todos los ámbitos a través de una actividad administrativa de inspección y control, pudiendo contribuir a la protección de los derechos del usuario"[9].

Ahora bien, "el carácter administrativo de la autoridad tutelar permite atribuirle también una función de divulgación o información pública del derecho que ayuda a su efectiva protección"[10]. Así, es evidente que "la existencia de una autoridad independiente de control forma parte del sistema del derecho fundamental a la protección de datos personales"[11]. Se constituye en uno de los pilares de todo marco jurídico, al momento de garantizar la tutela del derecho a la protección de

[7] Ramón Oró, *La Protección de datos Personales*, (Barcelona: Editorial UOC, 2015), 14.
[8] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 39.
[9] Antonio Troncoso, "El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional", *Revista Latinoamericana de Protección de Datos Personales*, Nro. 5 (2012). Disponible en: https://tinyurl.com/rvtguwp
**[10]** Muroi Bas, "La Agencia de Protección de Datos", 383.
**[11]** Lucas Murillo de la Cueva y Piñar, *El derecho a la autodeterminación informativa,* 108.

datos. En este marco, por ejemplo, el Tribunal de Justicia de la Unión Europea ha señalado que las autoridades de control se constituyen como "las guardianas" de los derechos y libertades fundamentales, que corresponden al tratamiento de datos de carácter personal. Como apunta el Tribunal, "su creación en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales"[12].

Salvo los casos que han recibido reconocimiento internacional, dentro de la Comunidad Andina, en el ámbito interamericano esta cuestión aún se encuentra en proceso de construcción y adaptación. Sin embargo, debemos destacar su relevancia, por cuanto la existencia de una institución independiente para la supervisión del marco de protección de datos significa uno de los más importantes principios dentro de un sistema jurídico. Así lo ha concretado la Guía legislativa de la OEA en 2021 al incluir como un nuevo principio, para la privacidad y la protección de datos personales, a las autoridades de protección de datos, considerando que los Estados "deberían establecer órganos de supervisión independientes, dotados de recursos suficientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos personales"[13].

En este punto, aclaramos que, inicialmente, la OEA no hizo referencia a la naturaleza y descripción de las funciones y facultades de las autoridades de control. La única prescripción, de la OEA, a través de la versión original de su Guía Legislativa, hizo referencia a que los Estados miembros "establezcan disposiciones, procedimientos o instituciones jurídicos, administrativos y de otros tipos que sean apropiados y eficaces para proteger la privacidad y las libertades individuales con respecto a los datos personales"[14]. Por otra parte también destacamos que los EPEI

[12] Cfr. Sentencia del Tribunal de Justicia de la Unión Europea (TJUE), asunto C-518/07, Comisión Europea contra la República Federal de Alemania, de 9 de marzo de 2010, apdo. 23.
[13] La Guía Legislativa de la OEA, que contiene los principios sobre privacidad y protección de datos personales, del Comité Jurídico Interamericano, fueron actualizados y aprobados en abril de 2021. Disponible en: http://www.oas.org/es/sla/cji/docs/CJI-doc_638-21.pdf
[14] Como señalaba la anterior versión de la Guía legislativa, "como no se observa un enfoque particular en los distintos Estados Miembros de la OEA, en estos principios se trata de no abordar la naturaleza

hacen especial mención a la naturaleza de las autoridades de control, considerando que en cada Estado "deberá existir una o más autoridades de control en materia de protección de datos personales con plena autonomía, de conformidad con su legislación nacional aplicable en la materia" –art. 42.1–[15].

Con estos antecedentes, este capítulo tiene por objeto: estudiar la actividad que desarrollan las autoridades de protección de datos personales; su naturaleza; organización; funciones y principales potestades, dentro del marco de regulación del derecho a la protección de datos. Para este fin, los proyectos de Ley de 2016 y 2019, la Ley Orgánica de Protección de datos Personales –LOPD– aprobada en mayo de 2021, en Ecuador; los Estándares de protección de datos personales para los Estados Iberoamericanos –EPEI– y la Guía Legislativa de la OEA serán los principales instrumentos que servirán de referencia. Lógicamente, especial importancia tendrá el análisis comparado del marco jurídico europeo, a partir de las disposiciones del Reglamento (UE) 2016/679 –RGPD– y de la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales –LOPDGDD–.

## 2. Naturaleza de las autoridades de control y supervisión

Considerada como una "magistratura informática"[16], por la naturaleza que compone una autoridad de control y supervisión, se define como un órgano de vigilancia del derecho a la protección de datos. En principio, tiene por objeto fortalecer el control jurisdiccional que ejerce el sistema de administración de justicia ordinaria, en lo que respecta a la protección de este derecho fundamental. Su actividad tiene especial

específica, la estructura, las autoridades y las responsabilidades de estas "autoridades responsables de la protección de datos".

[15] En este mismo sentido el RGPD señala que "cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento" –art. 54.1–.

[16] En nuestro concepto, esta denominación concentraría, plenamente, las virtudes y competencias que se desprenden de las actividades que, en la práctica, desarrollan las autoridades de control de datos personales. Cfr. Fermín, Morales Prats, "La tutela penal de la intimidad: privacy e informática", citado por Xavier Muroi Bas, en *Revista Administración Pública*: "La Agencia de Protección de Datos".

connotación, toda vez, que sobre estas autoridades "recae la responsabilidad de velar por el cumplimiento de la legislación nacional de protección de datos personales y por los derechos de las personas en relación con los ficheros y tratamientos de datos personales"[17].

En primer término, advertimos que las autoridades de protección de datos se consideran como instituciones que "llevan adelante una actividad de garantía del derecho fundamental a la protección de datos personales a través del cumplimiento de un conjunto de funciones"[18]. Estas funciones de garantía se concentran, esencialmente, en vigilar el cumplimiento del marco jurídico y tutelar el derecho de los titulares de los datos. Así, éstas fortalecen el marco integral de protección de datos, por medio, del aseguramiento de la confianza y seguridad jurídica de los ciudadanos. Precisamente, la LOPD define que la autoridad de protección de datos tiene como finalidad "proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales" –art. 4–. De esta manera, asumiendo que la actividad institucional que desarrollan las autoridades constituye uno de los pilares fundamentales del sistema de protección de datos; el control que manifiestan significa un mecanismo de protección y garantía vital, que los Estados deben considerar, dentro del esquema de regulación de la protección de datos. Por ello, "el control, aquella actividad desplegada con el afán de comprobar, inspeccionar o fiscalizar el desempeño propio o ajeno, constituye un quehacer no sólo necesario, sino indispensable en todo sistema jurídico organizado"[19].

Ahora bien, en el ámbito de la Unión Europea, el RGPD establece que las autoridades de control tienen la responsabilidad de supervisar la aplicación del Reglamento, "con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación

[17] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 244.
[18] Ibíd., 1769.
**[19]** Alberto Cerda Silva, "Mecanismos de Control en la Protección de Datos en Europa", *Revista Ius et Praxis*, Nro. 2 (2006): 221-251.

de datos personales" –art. 51.1–[20]. Asimismo, el RGPD considera, como una exigencia, que terceros países ofrezcan garantías de control independiente, plasmadas en el ejercicio de las autoridad de control[21].

En este marco, señalamos que el PLODP 2016 estimó que la Autoridad de Protección de Datos Personales –en adelante, autoridad de control– ejercería "la vigilancia y control para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley" –art. 11–. De igual manera, el PLODP 2019, a partir del principio de independencia de control, reconoció que "para el efectivo ejercicio del derecho a la protección de datos personales, el Estado ejercerá un control independiente, imparcial y autónomo, así como su regulación y sanción" –art. 21–. En este sentido, llamaba la atención que el PLODP 2019 hiciera referencia a que el Estado ejercería un control independiente, y no la Autoridad de Protección de Datos Personales. En todo caso, a la luz de esta última propuesta, en la LOPD el legislador ha concretado que "la Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción" –art. 10. m)–.

En el caso de la LOPDGDD, la Agencia Española de Protección de Datos –en adelante AEPD– "es una autoridad administrativa independiente de ámbito estatal (…) con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones" –art.

[20] Tal como señala el RGPD, "a fin de proteger a las personas físicas con respecto al tratamiento de sus datos personales y de facilitar la libre circulación de los datos personales en el mercado interior, las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión" –Considerando 123–.

[21] En este aspecto, el RGPD precisa que "el tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas" –Considerando 104– Así también señala que como normas relativas al establecimiento de la autoridad de control: "1. Cada Estado miembro establecerá por Ley todos los elementos indicados a continuación: a) el establecimiento de cada autoridad de control" –art. 54.1. a)–.

44.1–. Con relación a este aspecto, conviene apuntar que, el PLODP 2019 consideraba que la autoridad de control sería "una entidad de derecho público dependiente del poder ejecutivo con personería jurídica y gozará de autonomía administrativa y financiera" –art. 88–. Siendo una imprecisión manifestar que la autoridad estaría bajo la dependencia del ejecutivo, finalmente, la LOPD estatuye a ésta como una "autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte" –art. 4–.

Bajo estas primeras consideraciones, el ejercicio de las autoridades de control es cardinal, dentro del sistema jurídico para la tutela del derecho a la protección de datos, tanto en el ámbito nacional como internacional. Dentro de su naturaleza, una de las características de dichas autoridades tiene que ver con el carácter independiente con que estas instituciones ejercen sus actividades. Destacamos que el carácter independiente de las autoridades constituye un principio, dentro del marco de protección de datos, toda vez, que se han constituido como "unos entes públicos, dotados de independencia, con potestades de informe, inspección y sanción, entre otras, que velan por el respeto de todo este conjunto normativo"[22].

Por consiguiente, el principio de tutela independiente, –recogido en la CDFUE– en las autoridades de control, es esencial, por cuanto la actividad jurisdiccional que se ejerce, desde la función o poder judicial "se produce *ex post* y no permite un control preventivo que impida que se produzcan las vulneraciones al derecho fundamental a la protección de datos personales"[23]. No obstante, subrayamos que "la independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial"[24]. De esta forma, en virtud del carácter bifronte de las autoridades de control, –en cuanto a sus potestades administrativas, materialmente, jurisdiccionales y de prevención–, será importante

[22] Lucas Murillo de la Cueva y Piñar, *El derecho a la autodeterminación informativa,* 28.
[23] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1728.
[24] María José Blanco Antón, "Autoridades de control independiente (Arts. 55-59)", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018, 595.

evidenciar que la aplicación de la LOPD en Ecuador disponga de las suficientes garantías de independencia que enmarca el accionar de estas autoridades[25].

Si bien, el PLODP 2019, plasmado en la normativa de la LOPD, reconoció el carácter independiente de la autoridad de control; lamentablemente, el PLODP 2016 no describió que la autoridad podría actuar con plena independencia; *a contra sensu* de las potestades asignadas para la prevención y supervisión, en lo que respecta al derecho a la protección de datos personales[26]. La única previsión que señaló el art. 11 del PLODP 2016 fue que la autoridad de control estaría ejercida por la Dirección Nacional de Registros Públicos, adscrita al Ministerio de Telecomunicaciones y Sociedad de la Información. Tomando en cuenta que en este proyecto no se atribuía el carácter independiente de las autoridades de control; basándonos en la Ley del Sistema Nacional de Registros Públicos, que crea la Dirección Nacional de Registros Públicos –en adelante DINARDAP– estimábamos que esta Dirección se hubiera instituido como una autoridad de control, por cuanto constituye un "organismo de derecho público, con personería jurídica, autonomía administrativa, técnica, operativa, financiera y presupuestaria" –art. 30–

En este orden, respecto a la independencia y características de las autoridades, el Grupo Europeo de Protección de Datos del artículo 29 (GT29) sostiene que[27]:

---

[25] Como señala Antonio Troncoso, por ejemplo, las funciones que desarrollan la AEPD pueden ser consideradas como "materialmente jurisdiccionales" en virtud de las potestades de inspección, supervisión y sanción; y que, en suma, es lo que justifica que esta autoridad de control disponga de las garantías de independencia. Cfr. Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1729.

[26] Como señala el RGPD, "el establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa" –Considerando 117–. Asimismo, determina que "la independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial" –Considerando 118–.

[27] El Grupo Europeo de Protección de Datos se crea, a partir de lo dispuesto por el artículo 29 de la Directiva 95/46, con la finalidad de constituir un órgano consultivo independiente. Dicho órgano está integrado por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, así como por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y de igual manera, por un representante de la Comisión.

> Desde la década de 1970, el TEDH ha sostenido que cualquier interferencia con el derecho a la privacidad y protección de datos debe estar sujeta a un sistema de supervisión efectivo, independiente e imparcial que debe ser proporcionado por un juez u otro organismo independiente (por ejemplo, una autoridad administrativa o un cuerpo parlamentario)[28].

Refiriéndonos a los EPEI, las autoridades de control actuarán "con carácter imparcial e independiente en sus potestades" –art. 42.2–[29]. En este contexto, el principio de independencia es esencial dentro del marco integral para la protección de datos, por lo cual, el legislador –en el caso del PLODP 2016– debió concentrar mayores esfuerzos al momento de atribuir el carácter autónomo e independiente de esta autoridad. Por ello, enfatizamos que, si nuestro país pretende obtener reconocimiento internacional, el RGPD precisa que la evaluación de adecuación sobre niveles de protección se sujeta también a la "existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional" –art. 45.2. b)–[30].

Como refiere el GT29, citando al Tribunal de Justicia de la Unión Europea, "independientemente de la forma de supervisión independiente, la existencia de las

---

Entre las principales atribuciones del GT29, están: el estudio de la aplicación del marco legal de protección de datos de los Estados de la CE, la emisión de dictámenes, sobre el nivel de protección que tienen los Estados de la CE y de países terceros. Asimismo, según el RGPD, "el Comité debe sustituir al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por la Directiva 95/46/CE. Debe estar compuesto por el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de Protección de Datos, o por sus respectivos representantes (…) El Comité debe contribuir a la aplicación coherente del presente Reglamento en toda la Unión, entre otras cosas asesorando a la Comisión, en particular sobre el nivel de protección en terceros países u organizaciones internacionales, y fomentando la cooperación de las autoridades de control en toda la Unión. El Comité debe actuar con independencia en el cumplimiento de sus funciones" –Considerando 139–.

[28] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), Adopted on 13 April 2016, 9.

[29] Precisamente, los EPEI refieren que, "admitiendo la imperiosa necesidad de que cada Estado Iberoamericano cuente con una autoridad de control independiente e imparcial en sus potestades cuyas decisiones únicamente puedan ser recurribles por el control judicial, ajena a toda influencia externa, con facultades de supervisión e investigación en materia de protección de datos personales y encargada de vigilar el cumplimiento de la legislación nacional en la materia, la cual esté dotada de recursos humanos y materiales suficientes para garantizar el ejercicio de sus poderes y el desempeño efectivo de sus funciones" –Considerando 24–.

[30] Además, el RGPD señala que, los niveles de protección en las autoridades de control incluyen la responsabilidad de "garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros" –art. 45.2. b)–.

autoridades de supervisión constituye <un componente esencial de la protección de las personas en lo que respecta al procesamiento de datos personales>"[31]. Por tanto, dentro del PLODP 2016 no se podía obviar esta falta de previsión normativa, a condición de que se hubiera sistematizado, por vía del Reglamento de la Ley. De este modo, el carácter independiente de las autoridades de control "no es un privilegio ni una prerrogativa, sino que es una garantía para el ejercicio concreto de unas funciones, especialmente relacionadas con la actividad de las Administraciones Públicas"[32]. Por ello, advertimos que el modelo institucional de estas autoridades, y por el cual desempeñan sus facultades y potestades, "sirven para ejercer funciones jurídicas pero no para ejercer una actividad política"[33].

En este orden de ideas, subrayamos que:

> El TJUE ha señalado que «la mera posibilidad de que las autoridades del Estado puedan ejercer influencia política sobre las decisiones de las autoridades de control es suficiente para obstaculizar el ejercicio independiente de las funciones de estas». Por dos razones: la primera, porque podría dar lugar a una «obediencia anticipada» de las autoridades de control; la segunda, porque dado el papel de guardián de la protección de datos de las autoridades de control —la Sentencia habla de derecho a la intimidad—, esto exige que las autoridades de control «estén por encima de toda sospecha de parcialidad»[34]

Estas características, propias del principio de independencia de las autoridades de control, deben estar reflejadas y garantizadas, tanto en el marco legal que las regula como en la estructura orgánica que las compone. Como agrega el Tribunal de Justicia de la Unión Europea, "cuando se trata de un órgano público, el término «independencia» se refiere normalmente al estatuto que le garantiza la posibilidad de actuar con plena libertad, a resguardo de cualquier tipo de instrucciones o presiones"[35]. En todo caso, aclaramos que la observancia de este principio ha ocasionado algunas controversias, en lo que refiere a su adecuación en la legislación de protección de datos.

---

[31] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 9.
[32] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1733.
[33] Ibíd.
[34] Troncoso, "Autoridades de Control Independientes", 476.
[35] Cfr. Sentencia del Tribunal de Justicia de la Unión Europea (TJUE), asunto C-518/07, Comisión Europea contra la República Federal de Alemania, de 9 de marzo de 2010, apdo. 23.

> Se observa bastante celo en las legislaciones internas en lo tocante al nombramiento de quienes integran la autoridad de control, a las inhabilidades a que se ven afectos los mismos, a la inamovilidad de sus miembros, así como al otorgamiento de facultades reglamentarias y, quizá el punto que mayor esfuerzo demanda actualmente en la Unión Europea, la atribución de recursos materiales suficientes para el cabal desempeño de su cometido[36].

Por otra parte, "la independencia que requiere una autoridad de control consiste en no estar sometida a ninguna directriz jerárquica que pueda impedir el desempeño, con rigor y eficacia, de su función de control"[37]. En tal sentido, llamaba la atención lo previsto en el PLODP 2016 cuando se proponía que "la máxima autoridad del Ministerio de Telecomunicaciones y Sociedad de la Información será quien resuelva en última y definitiva instancia los recursos que se presenten" –art. 28–, ante la autoridad de control o DINARDAP. Aunque, tanto el Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información como la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), constituyen organismos públicos competentes, en materia del régimen general de telecomunicaciones; esta previsión no garantizaba, plenamente, el principio de independencia que a la autoridad de control le corresponde, en el marco del ejercicio de sus potestades[38]. En este caso, apuntamos que el RGPD considera que, institucionalmente, cada autoridad de control "serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción" –art. 52.2–. Así también los EPEI ponen de manifiesto que las autoridades de control "serán ajenas a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán orden ni instrucción alguna" –art. 42.2–.

En esta parte, hacemos referencia al respeto de unas garantías sustanciales de independencia, que se refieren a "la ausencia de una relación de jerarquía o de tutela administrativa, lo que impide que el Director de la Agencia de Protección de Datos reciba ordenes o directrices administrativas"[39]. Es decir, a la ausencia de "una

[36] Cerda Silva, "Mecanismos de Control en la Protección de Datos en Europa", 221-251.
[37] Ramón Oró, *La Protección de datos Personales*, 72.
[38] Véase el artículo 4 del Reglamento General a la Ley Orgánica de Telecomunicaciones.
[39] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1740.

relación de tutela y de órdenes e instrucciones en el ejercicio de sus funciones de las autoridades de control"[40].

> La independencia funcional de las autoridades de control, en el sentido de que no estén sujetas a instrucción alguna en sus funciones, como señala el TJUE, «es un requisito necesario para que dichas autoridades puedan ajustarse al criterio de la independencia». No obstante, «la independencia funcional no basta por sí sola para preservar a dichas autoridades de control de toda influencia externa»[41]

En suma, "la autonomía, término quizás más adecuado para definir la situación del ente, se hace patente en sus tres posibles aspectos o vertientes funcional, orgánica y financiera"[42]. En lo que respecta a esta parte, en el PLODP 2016 la autonomía o independencia orgánica y/o funcional de la autoridad de control, no lograba concretarse por las siguientes razones. Primero, la DINARDAP, al tenor de lo dispuesto por el art. 30 de la Ley del Sistema Nacional de Registro de Datos Públicos, acreditaría al menos autonomía financiera, pero no una independencia orgánica y/o funcional, en lo que respecta a su ejercicio de vigilancia y control sobre el orden jurídico de protección de datos personales. Y segundo, no existirían garantías sustanciales de independencia, en virtud del procedimiento para la aplicación de las sanciones. Además, las resoluciones de la DINARDAP, como una autoridad de control, no agotaban la vía administrativa y, consecuentemente, los recursos que se presentaren ante esta instancia estarían sujetas a la instrucción e influencia directa de la máxima autoridad del Ministerio de Telecomunicaciones y Sociedad de la Información. Esto es, bien del Ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información, o bien, de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)[43].

En todo caso, como hemos señalado, en el PLODP 2019 la independencia estaba definida de manera difusa, por cuanto se consideraba que el Estado ejercería un control independiente, cuando en realidad este ejercicio le corresponde a la

[40] Troncoso, "Autoridades de Control Independientes", 475.
[41] Ibíd.
[42] Muroi Bas, "La Agencia de Protección de Datos", 418.
[43] Sobre todo, debe tomarse en cuenta que los EPEI destacan que "Las decisiones de las autoridades de control únicamente estarán sujetas al control jurisdiccional, conforme a los mecanismos establecidos en la legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia y su derecho interno" –art. 42.5–.

autoridad de control. Asimismo, al haber señalado esta propuesta que la autoridad sería "dependiente" de la Función Ejecutiva, entendíamos que la autoridad de control no hubiera actuado con total independencia en el desempeño y ejercicio de sus poderes. Por ello, era preocupante que en ambos proyectos exista la ausencia de garantías formales de independencia en la estructuración de la autoridad de control. En todo caso, a la luz de la LOPD, dichas garantías se encuentran reconocidas a partir del principio de independencia del control –art. 4–. Desde este ámbito, advertimos que estas garantías:

> Se pueden clasificar en dos: garantías relativas a los miembros de la autoridad de control, como son la forma y requisitos para el nombramiento, la duración del mandato, la inamovilidad y la incompatibilidad, y que configuran un auténtico estatuto jurídico de los miembros de las autoridades de control; y las garantías relativas al funcionamiento de la propia autoridad de control, como son la autonomía de personal, presupuestaria y financiera y la disponibilidad de recursos humanos y económicos para el cumplimiento de sus funciones[44].

La inclusión de garantías de independencia, desde el punto de vista funcional, orgánico y financiero, son necesarias, toda vez, que permiten garantizar que su actuación se cumpla dentro de un marco de libertad y ajeno a toda influencia política o particular. Por tanto, tomando en cuenta, por un lado, la aprobación de la LOPD y, por otro, la Guía Legislativa de la OEA, se espera que se establezcan "los requisitos mínimos para cualquier tipo de protección de datos que las autoridades escojan, a fin de proporcionarles los recursos, el financiamiento y la pericia técnica que necesiten para desempeñar sus funciones eficazmente".

## 3. Las garantías formales de independencia

Un aspecto importante dentro de la independencia de las autoridades de control, como una garantía de la autonomía funcional, es la autonomía orgánica[45]. Para el cumplimiento de esta garantía, se requiere que la autoridad de control se instituya sobre una base transparente, de tal manera que quienes la integren se encuentren libres de presiones gubernamentales. Nos referimos a la observancia de las

[44] Troncoso, "Autoridades de Control Independientes", 476.
[45] Cfr. Muroi Bas, "La Agencia de Protección de Datos", 418.

garantías formales de independencia que "serían aquellas que se centran en el elemento personal como la inamovilidad del Director, la forma de nombramiento y el régimen de incompatibilidades –que configuran un auténtico Estatuto del Director de la Agencia–"[46]. Como apuntamos, "la legislación que fundamenta la creación de un órgano de control no sólo debe incluir disposiciones que garanticen de forma específica la independencia sino que la estructura organizativa específica de la autoridad también debe demostrar independencia"[47].

Así pues, mediante el reconocimiento de las garantías formales de independencia, se estatuyen, por ejemplo, las relativas "al funcionamiento de la propia autoridad de control como son la disponibilidad de recursos humanos y económicos para el cumplimiento de sus funciones y su autonomía de personal, presupuestaria y financiera"[48]. Además, dentro de la estructura de estas autoridades existen garantías que deben observarse, en virtud de que quienes integren su estructura orgánica desempeñen sus actividades, dentro del marco del principio de independencia. Entre otras garantías, nos referimos a la inamovilidad que se constituye como "el elemento más importante del estatuto jurídico de los miembros de las autoridades de control"[49]. Respecto a esta garantía, entendemos que "la principal garantía de independencia, sin cuya presencia no podemos considerar que una Administración pertenece a esta categoría, es la inamovilidad del órgano rector durante su período de mandato"[50]. En modelos de control y supervisión que han acreditado reconocimiento, la inamovilidad "inviste a los titulares de los órganos o autoridades de control del estatuto propio de los jueces, y por lo tanto de inamovilidad, tanto cuando se trata de órganos unipersonales como colegiados"[51].

> Esta garantía de inamovilidad es un elemento esencial para la independencia de las autoridades de control que (…) permite incluir a las Agencias de Protección de Datos dentro

[46] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1740.
[47] Agencia de los Derechos Fundamentales de la Unión Europea (Consejo de Europa), Manual de legislación europea en materia de la protección de datos, (Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2018), 127.
[48] Troncoso, "Autoridades de Control Independientes", 481.
[49] Ibíd., 479.
[50] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1741.
[51] Muroi Bas, "La Agencia de Protección de Datos", 409.

> de la categoría de las Autoridades independientes. Es la inamovilidad el elemento más importante del estatuto jurídico de los miembros de las autoridades de control[52].

Ahora bien, el Tribunal de Justicia de la Unión Europea expresa que la inamovilidad se encuentra, cardinalmente, vinculada con el principio de independencia, en cuanto al deber del Estado de respetar la duración del mandato de las autoridades de control y supervisión. En una de sus resoluciones ha señalado lo siguiente:

> Si cada Estado miembro tuviera la posibilidad de poner fin al mandato de una autoridad de control antes de que éste llegue al término inicialmente previsto sin respetar las normas y las garantías establecidas previamente en tal sentido por la legislación aplicable, la amenaza de tal terminación anticipada que en tal caso planearía sobre esa autoridad durante todo su mandato podría generar una forma de obediencia de ésta al poder político incompatible con dicha exigencia de independencia[53].

Asimismo, el GT29 refiere que "el Tribunal también recuerda que <la independencia funcional no es en sí misma suficiente para proteger a esa autoridad supervisora de toda influencia externa>"[54]. Por ello, con el objeto de afianzar, integralmente, el principio de independencia de las autoridades de protección, especial importancia comporta la previsión de garantías dentro de su estructura orgánica. Por ello, apuntamos que, "la autonomía hay que buscarla mejor en las garantías de inamovilidad, o de permanencia en el cargo (…) frente a las presiones gubernamentales, lo que le permite desarrollar su actividad incluso aunque pueda perjudicar los intereses del Gobierno"[55].

Respecto a este supuesto, el RGPD reconoce a la garantía de inamovilidad, señalando que "un miembro será destituido únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones" –art. 53.4–. En este sentido, el RGPD identifica unos supuestos tasados para la terminación del mandato, considerando que, "los miembros darán por concluidas sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria" –art. 53.3–. Asimismo, la LOPDGDD precisa que "la

[52] Troncoso, "Autoridades de Control Independientes", 478.
[53] Cfr. Sentencia del Tribunal de Justicia de la Unión Europea (TJUE), asunto C-288/12, Comisión Europea contra Hungría, de 8 de abril de 2014, apdo. 54.
[54] Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 10.
[55] Muroi Bas, "La Agencia de Protección de Datos", 419

Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por: a) Incumplimiento grave de sus obligaciones" –art. 48.5. a)–.

Esta garantía formal de independencia, en la estructura orgánica de la autoridad de control, se evidencia, a través de la previsión que permite el ejercicio continuo e ininterrumpido de su máximo representante. Por tanto, se limita el ámbito de intervención del Estado y tiende a respetar la libertad del ejercicio de su mandato, dentro del marco de protección del derecho a la protección de datos personales. Como agrega el Tribunal de Justicia de la Unión Europea:

> Los Estados miembros son libres de adoptar y modificar el modelo institucional que consideren más adecuado para sus autoridades de control. No obstante, deben en este marco velar por que no se limite la independencia de la autoridad de control exigida por el artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46, la cual implica la obligación de respetar la duración del mandato de tal autoridad, según ha quedado expuesto en el apartado 54 de la presente sentencia[56].

Las disposiciones señaladas dan cuenta de la previsión de las condiciones para la garantía de inamovilidad de las autoridades de control, mediante el respeto del tiempo de duración de su mandato, salvo la existencia de conductas irregulares dentro del ejercicio de sus funciones[57]. Estas condiciones resultan esenciales, toda vez que, como apreciamos, "otra garantía formal de independencia de los miembros de la autoridad de control es la existencia de un tiempo prefijado de mandato dentro del cual son inamovibles"[58].

Hasta aquí, advertíamos nuestra preocupación sobre la falta de previsión normativa que las propuestas de Ecuador evidenciaban en relación a las garantías formales, que requiere la autoridad de control. Ya señalábamos, inicialmente, el quebrantamiento –al menos en el PLODP 2016– de las garantías sustanciales, en virtud de que las decisiones de la autoridad de control no agotaban la instancia

[56] Cfr. Sentencia del Tribunal de Justicia de la Unión Europea (TJUE), asunto C-288/12, Comisión Europea contra Hungría, de 8 de abril de 2014, apdo. 60.
[57] Complementariamente, el RGPD determina que cada Estado miembro deberá establecer por Ley que "la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado" –art. 54.d)–.
[58] Troncoso, "Autoridades de Control Independientes", 477.

administrativa y, consecuentemente, se encontraban sujetas a una relación de jerarquía administrativa. Además, por lo que se refiere al PLODP 2019, éste no merecía ningún análisis, por cuanto no encontrábamos disposiciones relacionadas a este ámbito. En todo caso, finalmente, la LOPD ha determinado que el titular de la autoridad de control "ejercerá sus funciones por un período de 5 años y únicamente cesará en sus funciones por las causales establecidas en la Ley que regula el servicio público que le sean aplicables o por destitución, luego de enjuiciamiento político realizado por la Asamblea Nacional" –art. 77 *in fine*–.

Por un parte, siguiendo el tenor literal del art. 11 del PLODP 2016, la estructura orgánica de la autoridad de control hubiese respondido a la institucionalidad, por la cual, se encuentra compuesta la DINARDAP. Al señalarse que la autoridad sería ejercida por este organismo, forzosamente, debíamos acudir al marco jurídico que la regula. Así, conforme a lo dispuesto por el art. 30 de la Ley del Sistema Nacional de Registros Públicos, la Dirección de la DINARDAP es designada por el titular del Ministerio de Telecomunicaciones y Sociedad de la Información. En este sentido, según dispone el art. 85 de la Ley Orgánica de Servicio Público, quienes ejerzan esta Dirección se consideran como servidores públicos de libre nombramiento y remoción[59]. Ahora bien, respecto a los servidores públicos –excluidos de la carrera del servicio público–, la Ley Orgánica de Servicio Público expresa "exclúyase del sistema de la carrera del servicio público, a: Quienes tienen a su cargo la dirección política y administrativa del Estado" –art. 83. a)–. De conformidad a la norma expuesta, no existían garantías respecto a la inamovilidad de quien ostentara la representación de la autoridad de control. Así, advertíamos que, esto contradice al supuesto de que el poder gubernamental no puede manifestar un poder de remoción, dentro de las autoridades independientes de control y supervisión.

[59] Al respecto, la disposición indicada señala que "las autoridades nominadoras podrán designar, previo el cumplimiento de los requisitos previstos para el ingreso al servicio público, y remover libremente a las y los servidores que ocupen los puestos señalados en el literal a) y el literal h) del Artículo 83 de esta Ley. La remoción así efectuada no constituye destitución ni sanción disciplinaria de ninguna naturaleza".

En todo caso, a diferencia de la normativa internacional, las disposiciones de la LOPD dejan un amplio margen de supuestos para considerar que el titular de la autoridad de control pueda ser destituido. Por tanto, no aporta a la seguridad jurídica de la normativa de protección de datos cuando manifiesta que podrá ser cesado por las causales que le sean aplicables. Además, tampoco el legislador ha dejado claro cuáles serían las causas para que proceda su destitución. Naturalmente, son aspectos que deberán reformarse en la LOPD, por cuanto estos supuestos tasados tienen que estar previstos, únicamente, en la Ley que desarrolla el derecho fundamental a la protección de datos.

Por otra parte, dentro de la estructura orgánica, como una garantía formal, precisamos que debe observarse la forma en la que las autoridades de control deben ser nombradas. Nos referimos a otra garantía que se desprende de la autonomía o independencia orgánica, es decir, la garantía de *"*elección transparente*"* de los miembros que componen las autoridades de control.

> Evidentemente se trata éste de un ámbito donde existe un amplio margen de discrecionalidad y de apreciación a la hora de valorar si un candidato posee la cualificación y la idoneidad para ser nombrado, lo que limita el control jurisdiccional pero éste debe ejercerse en los supuestos en los que de manera clara y manifiesta el candidato propuesto no posee la titulación y la experiencia necesaria en el ámbito de la protección de datos personales, elementos éstos más reglados que la mayor o menor aptitud de un candidato que es siempre difícilmente valorable[60].

En este sentido, subrayamos que, "una cuestión discutida ha sido la necesidad de dotar de más garantías de independencia a la forma de nombramiento de los Directores de las Agencias"[61]. Precisamente, el art. 53.1 del RGPD reconoce que una condición aplicable a las autoridades de control es que sus miembros sean nombrados, mediante un procedimiento transparente[62]. Así también el RGPD dispone que "cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el

[60] Troncoso, "Autoridades de Control Independientes", 477.
[61] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1743.
[62] Como refiere el RGPD, "las condiciones generales aplicables al miembro o los miembros de la autoridad de control deben establecerse por Ley en cada Estado miembro y disponer, en particular, que dichos miembros han de ser nombrados, por un procedimiento transparente, por el Parlamento, el Gobierno o el jefe de Estado del Estado miembro, a propuesta del Gobierno, de un miembro del Gobierno o del Parlamento o una de sus cámaras, o por un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros" –Considerando 121–.

cumplimiento de sus funciones y el ejercicio de sus poderes" –art. 53.2–. Por tanto, lo que se pretende, a través de esta garantía es respetar la autonomía institucional en la elección y, en suma, contribuir al carácter independiente, sobre el cual las autoridades de control deben ejercer sus funciones.

Como señalamos, en el caso del PLODP 2016, entendíamos que la máxima autoridad y representante legal de la DINARDAP –como autoridad de control– hubiese sido designada por el titular del Ministerio de Telecomunicaciones y Sociedad de la Información[63]. Al constituirse como funcionarios o servidores públicos de libre nombramiento y remoción, no formaban parte de la carrera del servicio público y, consecuentemente, su designación no contemplaba ninguna política, norma, método y/o procedimiento. Más bien, su designación hubiese respondido a la voluntad política de quien ejerciera el Ministerio de Telecomunicaciones y Sociedad de la Información[64]. No obstante, pudo invocarse el control que ejerce la Función de Transparencia y Control Social, por cuanto, según lo dispuesto por la Ley que la regula, uno de sus objetivos es promover y desarrollar "el control de las entidades y organismos del sector público, y de las personas naturales o jurídicas del sector privado que presten servicios o desarrollen actividades de interés público, para que los realicen con responsabilidad, transparencia y equidad" –art. 4.1–[65].

Dentro de la garantía formal de nombramiento, además, podemos advertir la exigencia de que –quienes sean designados para ostentar la representación de la autoridad de control y supervisión– existan suficientes competencias para el

[63] Se entendería que el procedimiento de designación o elección en el PLODP 2019 seguiría un esquema similar toda vez que la autoridad de control sería dependiente de la Función Ejecutiva.
[64] El artículo 82 de la Ley Orgánica de Servicio Público señala que la carrera del servicio público. "Es el conjunto de políticas, normas, métodos y procedimientos orientados a motivar el ingreso y la promoción de las personas para desarrollarse profesionalmente dentro de una secuencia de puestos que pueden ser ejercidos en su trayectoria laboral, sobre la base del sistema de méritos".
[65] De conformidad a lo establecido en el art. 204 de la Constitución de la República, la Función de Transparencia y Control Social promoverá e impulsará el control de las entidades y organismos del sector público enumerados en su artículo 225, y de las personas naturales y jurídicas del sector privado que presten servicios o desarrollen actividades de interés público, para que los realicen con responsabilidad, transparencia y equidad; así como fomentará e incentivará la participación ciudadana, la protección del ejercicio y cumplimiento de los derechos; y prevendrá y combatirá la corrupción.

ejercicio de sus potestades. Así, “el establecimiento de determinadas condiciones de idoneidad profesional y de competencia para ser nombrado Director de las Agencia es otro elemento que puede facilitar no sólo la independencia (…) sino también el buen desempeño de la actividad”[66]. En este caso, por ejemplo, la LOPDGDD señala que la Presidencia de la Agencia Española de Protección de Datos y su Adjunto, “serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos” –art. 48.3–. Así, en el marco del PLODP 2016, debíamos remitirnos, nuevamente, a lo dispuesto por la Ley del Sistema Nacional de Registros Públicos. El art. 32 de esta Ley determina que como requisitos para ser Director Nacional de Registro se requiere:

1. Ser ecuatoriana o ecuatoriano
2. Tener título profesional de abogada o abogado.
3. Demostrar experiencia en el ejercicio profesional por un período mínimo de 5 años.
4. Encontrarse libre de inhabilidades para ejercer un cargo público; y,
5. Las demás que determina la Ley para el servicio público.

Evidenciando que estas garantías no se encontraban desarrolladas en el PLODP 2019, las condiciones de idoneidad y competencia, para la representación de la autoridad de control en el PLODP 2016, se concentraban, básicamente, en tener un título de abogado y demostrar experiencia en el ejercicio profesional, por un período mínimo de 5 años. En nuestro concepto, estos requisitos eran insuficientes para acreditar experiencia en la materia, por cuanto el título de abogado y la acreditación en el ejercicio profesional –en general–, no garantiza la existencia de conocimientos especializados en materia de protección de datos. Para hacer efectiva esta garantía, se requiere de profesionales que sean idóneos y con los conocimientos adecuados, cuya capacidad de gestión se demuestre, no solo, en virtud de su ejercicio profesional, sino en función de la experiencia que tengan en temas relacionados con la protección de datos personales.

En todo caso, ha sido la LOPD la que finalmente ha establecido que el titular de la autoridad de protección de datos o Superintendente de Protección de Datos sea “designado de acuerdo a lo establecido en la Constitución de la República, de la

[66] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1746.

terna que remita la Presidente o Presidente de la República, siguiendo criterios de especialidad y méritos; se sujetará a escrutinio público y derecho de impugnación ciudadana"; quien, además, "deberá ser un profesional del Derecho, de Sistemas de Información, de Comunicación o de Tecnologías, con título de cuarto nivel y experiencia de al menos 10 años con áreas afines a la materia objeto de regulación de esta ley" –art. 77–. Así, evidenciamos un importante reconocimiento sobre la forma en la que el titular de la autoridad de control deberá nombrarse; mediante un proceso transparente, sujeto al escrutinio público y derecho de impugnación ciudadana. Naturalmente, esta disposición pretende que el titular de la autoridad de control sea elegido en virtud de su experiencia y méritos, en materia de protección de datos personales.

Finalmente, otra garantía formal de las autoridades de control constituye la observancia del régimen de incompatibilidades, durante y posterior al ejercicio del cargo[67]. Al respecto, concretamos que:

> La aplicación del régimen de incompatibilidades tanto durante el ejercicio del cargo como una vez finalizado el tiempo de mandato es también una importante garantía no tanto de la independencia frente al poder político sino más bien de la dedicación a las funciones públicas durante el mandato y de la objetividad en el desempeño de las mismas[68].

El RGPD establece que "el miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no" –art. 52.3–[69]. Así también el art. 58.5. c) de la

[67] Al respecto, el RGPD apunta que "a fin de garantizar la independencia de la autoridad de control, sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones y no participar, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada. La autoridad de control debe tener su propio personal, seleccionado por esta o por un organismo independiente establecido por el Derecho de los Estados miembros, que esté subordinado exclusivamente al miembro o los miembros de la autoridad de control" –Considerando 121–.

[68] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1747.

[69] Así también el RGPD precisa la obligatoriedad de que éstas sean establecidas por Ley. Por ejemplo, se señala: "a) el establecimiento de una autoridad de control; b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control; c) las normas y los procedimientos para el nombramiento; d) la duración del mandato; e) el carácter renovable o no del mandato; f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo" –art. 54.1–.

LOPDGDD dispone que la incompatibilidad será una causal para la separación –antes de la expiración de su mandato– del Presidente y el Adjunto de la AEPD.

A la falta de una previsión normativa en la LOPD, la única norma que regula la incompatibilidad, en el ejercicio de un cargo público, es la Ley Orgánica de Servicio Público. Así, el representante o Director de la autoridad de control estaría sometido a la prohibición contemplada en el art. 12 de dicha Ley, por el cual, "ninguna persona desempeñará, al mismo tiempo, más de un puesto o cargo público, ya sea que se encuentre ejerciendo una representación de elección popular o cualquier otra función pública".

Como queda evidenciado, la LOPD, plantea de manera difusa los elementos que configuran la independencia de la autoridad de control, a partir de las garantías formales que se señalan. Precisamente, mediante este estudio pretendemos identificar las virtudes y los defectos, de tal manera, que nuestro país pueda articular un marco integral para la protección de datos personales. Así, con el objeto de afianzar el principio de independencia de la autoridad de control, consideramos necesario que la LOPD, en su reglamentación, deberá recoger las garantías formales –inamovilidad, forma de nombramiento e incompatibilidad–, que hasta ahora se han analizado.

En todo caso, un modelo de estas previsiones en la región también puede significar las garantías señaladas en el art. 42.3 de los EPEI, en donde se sugieren que las autoridades de control deben contar con las garantías formales antes descritas. En este sentido, se establece que:

> El miembro o los miembros de los órganos de dirección de las autoridades de control deberán contar con la experiencia y aptitudes, en particular respecto al ámbito de protección de datos personales, necesarios para el cumplimiento de sus funciones y el ejercicio de sus potestades. Se nombrarán mediante un procedimiento transparente en virtud de la legislación nacional aplicable y únicamente podrán ser removidos por causales graves establecidas en el derecho interno de cada Estado Iberoamericano, conforme a las reglas del debido proceso.

Según este instrumento, debe establecerse la garantía de inamovilidad y procedimiento para la designación de quien ejerce la autoridad de control. Sin embargo, quedaría pendiente plantear la regulación sobre el régimen de

incompatibilidades, en virtud de las disposiciones del RGPD[70]. Conforme a la situación en Ecuador, la ausencia de presupuestos que aseguren este objetivo, no puede suplirse, mediante la interpretación de la Ley que regula a la autoridad de control. Como señala la Guía legislativa para los Estados Miembros de la OEA; la sistematización del orden jurídico para la protección de datos exige la articulación de instituciones jurídico-administrativas, que se materialicen en las denominadas autoridades de control y supervisión[71]. Como apreciaremos, la falta de normativa en la LOPD, sobre la estructura y naturaleza de las autoridades de control, no responde a las necesidades y fines que exige el marco de regulación para la protección de datos personales. Por tanto, advertimos que, podría ponerse en riesgo las actividades de control independiente. En todo caso, los instrumentos internacionales que quedan anotados deben significar el punto de partida, en Ecuador, para articular un marco jurídico equilibrado.

### 3.1 Referencia especial a la autonomía financiera

Dentro del principio de independencia de las autoridades de control, un elemento constitutivo que define su actividad es la autonomía financiera. Adicional a las garantías formales que hemos precisado también debe considerarse "aquellas que se refieren a elementos financieros o burocráticos como la autonomía personal, la autonomía presupuestaria y la autonomía organizativa"[72]. De este modo, "un

[70] Los EPEI refieren que las directrices orientadoras que se señalan en esta Declaración se formulan: "teniendo en cuenta que la Unión Europea ha adoptado un nuevo marco normativo en la materia, con el objetivo de modernizar sus disposiciones y garantizar mayor solidez y coherencia en la protección efectiva del derecho fundamental a la protección de datos personales en la Unión Europea y con el fin de generar confianza en la sociedad en general y, a su vez, facilitar el desarrollo de la economía digital, tanto en su mercado interior como en sus relaciones globales; marco normativo que se posiciona como un referente obligado y determinante para la elaboración de las legislaciones nacionales de protección de datos en Iberoamérica" –Considerando 8–.

[71] Adicionalmente, los EPEI reconocen que dentro de los Estados Iberoamericanos existe una falta de armonización dentro del marco jurídico regional para la protección de datos personales. Al respecto, se menciona que "reconociendo que existe una falta de armonización en los Estados Iberoamericanos respecto al reconocimiento, adopción, definición y desarrollo de las figuras, principios, derechos y procedimientos que dan contenido al derecho a la protección de datos personales en sus legislaciones nacionales" –Considerando 9–.

[72] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1740.

elemento necesario, tanto para la independencia de las autoridades de control como para el correcto cumplimiento de sus funciones, es que éstas cuenten con los medios humanos, técnicos, financieros y organizativos para poder ejercer sus poderes"[73]. Así, solamente, puede hablarse de independencia de las autoridades de control cuando exista, entre otras garantías, un elemento patrimonial y de financiación propia para el cumplimiento de sus potestades de control, supervisión y, en fin, de tutela del derecho a la protección de datos[74].

Este argumento tiene pleno fundamento, toda vez que, para el correcto funcionamiento y plena ejecución de las potestades de cualquier institución estatal, se requieren de los suficientes y necesarios medios materiales y económicos[75]. En este sentido, "puedes ser independiente, o al menos querer serlo, pero las carencias presupuestarias o de plantilla pueden limitar la actividad de inspección y, por tanto, la independencia en el ejercicio de sus funciones"[76].

Sobre esta garantía o elemento patrimonial de las autoridades de control, los arts. 52.4 y 52.5 del RGPD precisan que:

> 4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité; 5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada[77].

---

[73] Troncoso, "Autoridades de Control Independientes", 481.

[74] Cfr. Ana Herrán Ortiz, *El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales*, (Madrid: Dykinson, 2004), 326.

[75] Como señala el RGPD, "todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus funciones, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión. Cada autoridad de control debe disponer de un presupuesto anual público propio, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional" –Considerando 120–.

[76] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1748.

[77] Adicionalmente, el RGPD advierte que: "todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus funciones, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión. Cada autoridad de control debe disponer de un presupuesto anual público propio, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional" –Considerando 120–.

Ahora bien, los EPEI también subrayan que “las autoridades de control deberán contar con los recursos humanos y materiales necesarios para el cumplimiento de sus funciones” –art. 42.6–. La garantía de contar con recursos suficientes, para el cabal cumplimiento de las funciones y potestades de las autoridades de control, conlleva a que, de esta manera, exista una actividad fiscalizadora que, desde el Estado, permita ejercer los principios de transparencia, rendición de cuentas y control social. Así, destacamos que, “una Administración Independiente no deja de ser una Administración y, por tanto, está sometida al ordenamiento jurídico (…) Es decir se entiende que la remisión es a los principios generales de la legislación y no a los aspectos competenciales”[78].

Desde esta perspectiva, el RGPD dispone que, las autoridades de control estarán sujetas a “un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente” –art. 52.6–. En este caso, el control es financiero, a partir de la asignación presupuestaria, mas no, sobre el ejercicio de sus potestades de supervisión y control. Por otra parte, la LOPDGDD determina que “la Agencia Española de Protección de Datos elaborará y aprobará su presupuesto y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado” –art. 46.1–. Por ello, reconocemos que “dejar todas las competencias de personal y de presupuestos en manos de la Administración General –que es objeto de control y supervisión– puede condicionar la efectividad de su actividad y afectar a su independencia”[79].

Esta facultad permitiría que la AEPD tenga la posibilidad de una “redistribución de créditos a nivel de programa, lo que permite una gran agilidad, evitando el control ejercido –que puede ser entendido como un control político– por otro órgano de la Administración General”[80]. En esta parte, enfatizamos que el Tribunal de Justicia de la Unión Europea determina que “la atribución de los medios humanos y materiales que necesita tal autoridad de control no debe impedir que ejerza sus funciones «con

[78] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1755.
[79] Ibíd., 1749.
[80] Ibíd., 1753.

total independencia» en el sentido del artículo 28, apartado 1, párrafo segundo, de la Directiva 95/46"[81]. Al mismo tiempo, este Tribunal aclara que el término «independencia» viene reforzado por el adjetivo «total»; "lo que implica una facultad de decisión exenta de toda influencia externa a la autoridad de control, ya sea directa o indirecta"[82].

Sin establecer la LOPD disposiciones sobre la autonomía financiera, corresponde analizar las propuestas que se presentaron. El PLODP 2019 señalaba, únicamente, que la autoridad de control gozaría "de autonomía administrativa y financiera" –art. 88–. Además, sin haber advertido una previsión normativa dentro del PLODP 2016, por medio de las disposiciones de la Ley del Sistema Nacional de Registros Públicos, la autoridad de control, al menos, pudo acreditar autonomía financiera. Como se prevé en esta Ley, la DINARDAP posee "autonomía administrativa, técnica, operativa, financiera y presupuestaria, adscrita al Ministerio de Telecomunicaciones y Sociedad de la Información" –art. 30–[83].

Si bien, existe un reconocimiento sobre la autonomía financiera, la autoridad de control estaría bajo una influencia indirecta del Ministerio de Telecomunicaciones y Sociedad de la Información. En este contexto, advertimos que "existen otras garantías formales como la autonomía de personal, la autonomía presupuestaria y la autonomía organizativa, que facilitan, de manera indirecta, la independencia de estas instituciones. Hay muchas formas indirectas de condicionar la actividad de una Administración Independiente"[84]. Así, una forma indirecta de condicionar la actividad de la autoridad de control sería, en primer término, encontrarse adscrita al Ministerio de Telecomunicaciones y Sociedad de la Información. Esta presunción,

[81] Cfr. Sentencia del Tribunal de Justicia de la Unión Europea (TJUE), asunto C-614/10, Comisión Europea contra la República de Austria, de 16 de octubre de 2012, apdo. 58. Conviene aclarar que el artículo 28, apartado 1, de la Directiva 95/46, titulado «Autoridad de control», establece: «Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. Estas autoridades ejercerán las funciones que les son atribuidas con total independencia.»
[82] Cfr. Sentencia del Tribunal de Justicia de la Unión Europea (TJUE), asunto C-518/07, Comisión Europea contra la República Federal de Alemania, de 9 de marzo de 2010, apdo. 19.
[83] Debe considerarse que según el artículo 31.3 de la Ley citada corresponde a la DINARDAP elaborar su propio presupuesto.
[84] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1748.

se deriva de la falta de regulación normativa relacionada con los presupuestos que enmarcan la garantía de independencia de las autoridades de control[85]. En todo caso, precisamos que, esta garantía está encaminada a impedir que la gestión presupuestaria –de los medios con los que requiere ejercer las actividades de control y supervisión– pueda debilitar la actividad de tutela, que las autoridades de control están llamadas a cumplir.

### 4. Funciones de la autoridad de control

Las competencias y potestades de la autoridad de control se enmarcan en desarrollar "una actividad de garantía del derecho fundamental a la protección de datos personales a través del cumplimiento de un conjunto de funciones"[86]. Este conjunto de funciones "pueden clasificarse atendiendo a los diferentes fines a que responden, ya que las diversas actuaciones de la Agencia tenderán en cada caso a dar respuesta a las necesidades de tutela y control en la protección de datos personales"[87]. Siguiendo la experiencia desarrollada por la AEPD, distinguimos funciones en el ámbito normativo; de control de ficheros; de tutela de derechos y de ejercicio de la potestad sancionadora; de publicidad y registro de ficheros; y de promoción del derecho a la autodeterminación informativa[88]. En este orden, considerando la normativa de protección de datos de Ecuador, en los siguientes apartados, conceptualizaremos el contenido de las funciones que las autoridades de control y supervisión desarrollan en el marco de la garantía de este derecho fundamental[89].

---

[85] Podría ser importante que, en el caso de Ecuador, la actividad de supervisión y control que cumpliera la autoridad de control se normalice, a través de un Estatuto que permita desarrollar en conjunto las garantías formales y sustanciales del principio de independencia.

[86] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1769,1770.

[87] Ana Herrán Ortiz, *El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales*, 331.

[88] Cfr. Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1772.

[89] Puede considerarse también otros criterios sobre las funciones que desempeñan las autoridades de control y supervisión. Así, por ejemplo, se señala que las funciones de la autoridad de protección de datos se concentran en los ámbitos de control, inspección, sanción, normativo, tutela de derechos, publicidad, cooperación normativa y cooperación internacional e interregional. Cfr. Ana Herrán Ortiz, *El derecho a la intimidad en la nueva Ley orgánica de protección de datos personales*, 332, 333, 334. Por otra parte, se destaca que las funciones de las autoridades pueden sistematizarse en actividades

A. Función normativa o reguladora

La función normativa o reguladora de la autoridad de control comprende desarrollar "criterios y medidas concretas en materia de calidad de datos –finalidad, tipología de datos, plazo de cancelación–, información, consentimiento, posibles cesiones, etc., que permiten materializar la protección de datos en los distintos tratamientos"[90]. Así, en contextos jurídicos comparados, el marco legal de protección de datos establece que las autoridades de control dispongan de un conjunto de potestades o facultades de carácter reguladora, que facilite la aplicación de la legislación de protección de datos. En este ámbito, la autoridad de control "dispone habitualmente de facultades normativas, ya sea de orden general, que se concreta en disposiciones reglamentarias, o bien particular, mediante la emisión dictámenes u pronunciamientos específicos"[91]. Por tanto, "parece razonable también que las Administraciones Independientes puedan disponer de una función normativa que complete la normativa legal y reglamentaria, siempre que esta función disponga de la necesaria cobertura legal"[92].

El art. 89 del PLODP 2019 ha precisado algunas de estas facultades normativas en la LOPD. Por ejemplo, "emitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y garantizar el ejercicio del derecho a la protección de datos personales" –art. 76.5–; "dictar cláusulas estándar de protección de datos, así como verificar el contenido de las cláusulas o garantías adicionales o específicas" –art. 76.8; "emitir directrices para el diseño y contenido de la política de tratamiento de datos personales" –art. 76.12–; "establecer directrices para el análisis, evaluación y selección de medidas de seguridad de los datos personales" –art. 76.13–; y "publicar periódicamente una guía de la normativa relativa a la protección de datos personales" –art. 76.15–.

---

de difusión; asistencia y promoción; registro; inspección; facultades sancionadoras; facultades cautelares; facultades normativas; y cooperación Internacional. Cfr. Cerda Silva, "Mecanismos de Control en la Protección de Datos en Europa", 221-251.

[90] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1775.

[91] Cerda Silva, "Mecanismos de Control en la Protección de Datos en Europa", 221-251.

[92] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1774.

Si bien, el art. 12 del PLODP 2016 no hizo referencia a las atribuciones de carácter normativo; la DINARDAP se presentaba como una autoridad de protección de datos. Del texto de la norma indicada, la DINARDAP pudo ejercer, complementariamente, algunas atribuciones señaladas en otros cuerpos legales. Así, conforme a lo previsto en la Ley del Sistema Nacional de Registros Públicos, correspondía a la ANPDP "dictar las resoluciones y normas necesarias para la organización y funcionamiento del sistema" –art. 31.2–; y así también "promover, dictar y ejecutar a través de los diferentes registros, las políticas públicas a las que se refiere esta Ley, así como normas generales para el seguimiento y control de las mismas" –art. 31.4–. La DINARDAP está encargada de presidir el Sistema Nacional de Registros Públicos –art. 31.1–. Al haberse considerado en el PLODP 2016 que esta Dirección ejercería las funciones de ANPDP, la función normativa o reguladora en materia de protección de datos estuvo, subsidiariamente, ostentada según lo prescrito en la Ley del Sistema Nacional de Registros Públicos.

La concreción de esta función permite que la autoridad de control pueda desarrollar dictámenes, criterios, medidas de seguridad y pronunciamientos específicos, orientados a proteger el tratamiento de la información personal. Frente a la legislación de protección de datos, las facultades normativas facilitan la comprensión de una legislación que, algunas veces, puede resultar compleja y abstracta y que, en todo caso, por medio, de su potestad reguladora "salvan sus omisiones y hace frente a la obsolescencia normativa resultante de las permanentes innovaciones introducidas en el sector"[93].

Por ejemplo, la LOPDGDD dispone que corresponde a la AEPD "ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento" –art. 47–. En este sentido, el RGPD, dentro de esta tipología de funciones, precisa que las autoridades de control pueden: "dictaminar y aprobar los códigos de conducta que den suficientes garantías" –art. 57.1. m)–; "elaborar y publicar los criterios para la acreditación de organismos de supervisión de los códigos de conducta" –art. 57.1. p)–; "emitir, por iniciativa propia o previa solicitud,

[93] Cerda Silva, "Mecanismos de Control en la Protección de Datos en Europa", 221-251.

dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales" –art. 58.3. b)–; y "aprobar los criterios de certificación" –art. 58.3. f)–. En este orden, los EPEI consideran que el marco jurídico, que resulte aplicable para la protección de datos, deberá garantizar que las autoridades de control cuenten con "suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de ésta, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales" –art. 42.4–.

Por consiguiente, en esta parte, destacamos que las autoridades control deben contar con poderes de resolución necesarios para formular recomendaciones e instrucciones. Así, sobre esta función normativa o reguladora –concretada, mediante recomendaciones e instrucciones–, aclaramos que:

> Dentro de la función normativa de la Agencia de Protección de Datos hay que distinguir la Instrucción que tiene un carácter vinculante y que aporta alguna novedad a este ordenamiento, de la Recomendación, que incluye criterios y buenas prácticas a modo de recordatorio del cumplimiento de la legislación en un sector específico[94].

La función normativa o reguladora que ejercen las autoridades de control, estaría "subordinada a la Ley y a la normativa reglamentaria y centrada en la aplicación de los principios y derechos de protección de datos personales a supuestos y ámbitos concretos"[95]. Al parecer, esta función –en el caso del PLODP 2016– tuvo una tarea pendiente. Si bien, pudo ejercerse, mediante las prescripciones de la Ley del Sistema Nacional de Registros Públicos, para concretar parámetros adecuados de protección de datos; era indispensable contar con una legislación equilibrada, uniforme y coherente, que responda a estándares internacionales y al desarrollo que plantean las nuevas tecnologías.

[94] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1774.
[95] Ibíd., 1777

B. Función de control de ficheros, de tutela de derechos y de ejercicio de la potestad sancionadora

Las autoridades de control, por su propia naturaleza, constituyen un ente de supervisión y tutela del derecho a la protección de datos. Estas funciones se acompañan de una serie de facultades, que permiten imponer sanciones, como resultado del incumplimiento del marco legal previsto para la garantía de este derecho. En este orden, las autoridades de control tienen la responsabilidad de "investigar las posibles vulneraciones de la normativa de protección de datos dentro de su ámbito competencial, investigación que puede ser consecuencia de una propuesta de tratamiento notificado a la Agencia o de una queja del titular de los datos"[96]. Por ello, consideramos que "sólo si la Agencia desarrolla de manera efectiva esta función de control y tutela de derechos puede garantizarse el cumplimiento de los principios y de los derechos de protección de datos personales"[97].

El PLODP 2016 atribuyó a la autoridad de control la función de "velar por el cumplimiento de la legislación en materia de protección de datos personales" –art. 12.1–. Dentro de este conjunto de facultades –que se simplifican en cuidar el cumplimiento de la legislación–; en primer término, la actividad de control conllevaba "una supervisión sobre los tratamientos de datos personales. Por este motivo, la Agencia lleva a cabo, a través de la inspección de datos, las funciones inherentes a la potestad de inspección recabando cuantas informaciones necesite"[98]. Además, a la luz del art. 89 del PLODP 2019, la LOPD ha precisado que le corresponde a la autoridad de control: "garantizar a todos los ciudadanos la protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley y en su reglamento de aplicación" –art. 76–; "ejercer la supervisión, control y evaluación

[96] Troncoso, "Autoridades de Control Independientes", 486.
[97] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1789.
[98] Ibíd., 1790

de las actividades efectuadas por el responsable y encargado del tratamiento de datos personales" –art. 76.1–.

Por medio de la actividad de control, lo que se pretende es mantener una constante evaluación sobre el nivel de cumplimiento de la legislación de protección de datos y, en todo caso, asignarle a la autoridad control potestades que le permitan sancionar su incumplimiento. Lógicamente, para el ejercicio de estas funciones "la autoridad de supervisión deberá tener acceso a todos los datos personales y a la información que resulte necesaria para su investigación, así como acceso a todos los locales en los que un responsable del tratamiento conserve la información relevante[99].

Por otra parte, el RGPD reconoce como una función de la autoridad de control "facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, además, cooperar a tal fin con las autoridades de control de otros Estados miembros" –art. 57.1. e)–. Asimismo, "tratar las reclamaciones presentadas por un interesado o por un organismo, organización, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación" –art. 57.1. f)–. Finalmente, la LOPDGDD faculta a la AEPD a "supervisar la aplicación de esta Ley orgánica y del Reglamento (UE) 2016/679" –art. 47–.

Llamaba la atención que el PLODP 2016 no acreditara a dicha autoridad la facultad de controlar la aplicación de la Ley y, más bien –sentido general– señale, únicamente, la función de velar por su cumplimiento. No obstante, este proyecto de Ley facultaba a la autoridad de control "realizar la vigilancia y control de las bases o bancos de datos, ficheros o archivos físicas o digitales" –art. 12.9–. Así, la función de control de las autoridades de protección de datos implica que estén dotadas de "facultades de inspección, las que incluyen el requerimiento de informes y

[99] Agencia de los Derechos Fundamentales de la Unión Europea (Consejo de Europa), Manual de legislación europea en materia de la protección de datos, 130.

antecedentes de los responsables de base o registros de datos, así como el ingreso y registro de los establecimientos y equipos en que se realizan las operaciones"[100].

Dentro de este apartado, además hacemos referencia a la función sobre la tutela de los derechos. Nos referimos, especialmente, a la garantía de los derechos ARCO. En este aspecto, apuntamos que, "le corresponde también a las Agencias de Protección de Datos velar por los derechos de acceso, rectificación y cancelación que la legislación atribuye a los ciudadanos para controlar de manera efectiva su información personal"[101]. Desde este punto de vista, el PLODP 2016 advirtió que "las actuaciones contrarias a lo dispuesto en la presente Ley serán objeto de acción constitucional de *habeas data*, conforme lo establecido en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional" –art. 13–. Por tanto, conjuntamente, con las funciones que se encontraban enmarcadas en el art. 12, la única vía que tenían los ciudadanos para concretar el control de su información personal –por medio de los derechos de actualización, rectificación, eliminación, anulación o confidencialidad–, era la jurisdiccional, por medio del *habeas data*. En este punto, anotamos que, sobre la base del art. 89 del PLODP 2019, la LOPD ha reconocido que le corresponde a la autoridad de control "conocer, sustanciar y resolver los reclamos interpuestos por el titular o aquellos iniciados de oficio, así como aplicar las sanciones correspondientes" –art. 76.3–.

Llegados a este punto, conviene preguntarnos si es relevante que las autoridades de control, puedan ejercer la protección de estos derechos y, consecuentemente, materializar las potestades de tutela de derechos, por vía administrativa. Al respecto, precisamos que –de conformidad al marco jurídico internacional que hasta ahora hemos estudiado–, estas facultades no encuentran ninguna limitación o restricción, toda vez, que una de las principales funciones de las autoridades de control se concentra, fundamentalmente, en conceder a los ciudadanos el ejercicio de los derechos ARCO y, en este sentido, actuar en calidad de una magistratura.

[100] Cerda Silva, "Mecanismos de Control en la Protección de Datos en Europa", 221-251.
[101] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1794.

Como hemos referido, la LOPDGDD faculta a la AEPD para ejercer las funciones señaladas en el art. 57 del RGPD. Así, el RGPD dispone que las autoridades de control "facilitarán la presentación de las reclamaciones contempladas en el apartado 1, letra f)" –art. 57.2–; es decir, "tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación"[102]. Finalmente, –como parte de los poderes correctivos–, el RGPD faculta "la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18" –art. 58.2.g)–, que regulan el derecho de rectificación; derecho de supresión o derecho al olvido; y derecho a la limitación del tratamiento. En este sentido, recordemos que los EPEI también precisan que las autoridades de control cuenten con otros poderes que "resulten necesarios para garantizar el efectivo cumplimiento de ésta, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales" –art. 42.4–. En este orden de ideas, señalamos que:

> Esta actividad coercitiva o de *enforcement* implica la función de investigación sobre el cumplimiento de la legislación por parte de responsables y encargados del tratamiento que puede iniciarse, bien en virtud de una reclamación presentada ante la autoridad de control o bien, de oficio o a instancia de otra autoridad[103].

Uno de esos poderes es que, las autoridades puedan conocer las reclamaciones que se desprendan del ejercicio de los derechos de acceso, rectificación y cancelación. En todo caso, la función de tutela de estos derechos se concreta "cuando estos derechos no sean respetados por el responsable del fichero, a diferencia de la actividad de inspección, por su propia naturaleza, no puede ser iniciada de oficio por la Agencia sino que requiere la solicitud del titular del derecho"[104]. Por consiguiente, observando las disposiciones del RGPD, advertimos que:

> Además, la autoridad de control no se limita a una actividad pasiva de tramitación, sino que, al igual que el responsable de tratamiento se rige por un principio de responsabilidad proactiva —art. 5.2—, cada autoridad de control «facilitará la presentación de las reclamaciones […] mediante medidas como un formulario de presentación de reclamaciones

[102] El citado RGPD menciona que, las reclamaciones podrán ser presentadas "mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación" –art. 57.2–.
[103] Troncoso, "Autoridades de Control Independientes", 499.
[104] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1794.

que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación»[105].

Bajo estas precisiones, la forma en la que se presentaba el PLODP 2016 era preocupante. Las autoridades de control deben contar con la suficiente capacidad de intervención, de tal manera que, "las quejas y reclamaciones de los ciudadanos, cuando consideren que sus libertades han sido vulneradas como consecuencia de incumplimientos del derecho a la protección de datos personales, sean convenientemente atendidas"[106]. Si bien, el derecho de conocer, actualizar y rectificar los datos personales, frente a su tratamiento inadecuado; así como, de oponerse y solicitar la supresión de los datos se encontraban, formalmente, reconocidos en el art. 6 del PLODP 2016. La función de tutela –por vía administrativa– de estos derechos, mediante la atención de reclamaciones y quejas se encontraba ausente en este proyecto. Como precisaba el PLODP 2016, las reclamaciones que hubiesen surgido de actuaciones, contrarias a la legislación de protección de datos, habría sido objeto de la acción de *habeas data*.

Finalmente, en relación a la función que permite ejercer la potestad sancionadora, la autoridad de control y supervisión está facultada para "imponer sanciones administrativas –tales como multas y restricciones temporales para el tratamiento de datos– cada vez que se cerciora de la ocurrencia de actos u omisiones que importen una infracción a las disposiciones legales y reglamentarias vigentes"[107]. En este caso, el art. 22 del PLODP 2016 determinó que la autoridad de control tendría dichas facultades. Esta potestad se encontraba afianzada en la atribución de "determinar la responsabilidad de las infracciones e imponer las sanciones a los responsables del tratamiento y responsables de las bases o bancos de datos, ficheros y archivos, previo el debido proceso correspondiente" –art. 12.8–. Ahora bien, sobre la base del art. 89 del PLODP 2019, la LOPD ha determinado que la autoridad de control podrá "ejercer la potestad sancionadora respecto de responsables, delegados, encargados y terceros" –art. 76.2–.

[105] Troncoso, "Autoridades de Control Independientes", 500.
[106] Ramón Oró, *La Protección de datos Personales*, 70,71.
[107] Cerda Silva, "Mecanismos de Control en la Protección de Datos en Europa", 221-251.

Bajo estas consideraciones, precisamos que "la potestad sancionadora es un complemento necesario de la función de control"[108] y, consecuentemente, el procedimiento sancionador se aplica, una vez, determinado el cometimiento de una infracción, por parte de los responsables del tratamiento. En este sentido, también el art. 42. 4 de los EPEI precisan que las autoridades de control puedan disponer de suficientes poderes de sanción, que permitan hacer efectivo el cumplimiento de la legislación de protección de datos. Como advertimos, según el art. 47 de la LOPDGDD, la autoridad de control podrá ejercer las potestades previstas en el artículo 58 del RGPD. Precisamente, el RGPD determina que las autoridades de control disponen de poderes correctivos, tales como: sancionar con una advertencia a los responsables o encargados del tratamiento, cuando "las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento" y así también sancionar con apercibimiento cuando "las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento" –art. 58.2–[109].

Por tanto, en el ámbito europeo:

> La protección efectiva de los datos personales en la Unión no sólo exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de los responsables de tratamiento sino también que los Estados miembros «reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes»[110].

Sobre estas consideraciones, parecía que el PLODP 2016 afianzaba, al menos, la función sancionadora de la autoridad de control, a partir de la regulación que contemplaba en el art. 23, sobre las infracciones, tanto leves como graves, que afectaran al tratamiento y a las libertades relativas al derecho a la protección de datos personales. Sin embargo, el procedimiento sancionatorio resultaba incierto, por cuanto el PLODP 2016 mencionaba que la autoridad de control iba a determinar "las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación con la gravedad y extensión de la violación y de

[108] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1792.
[109] Recordemos que el RGPD prevé el reconocimiento de "poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes" –Considerando 11–.
[110] Troncoso, "Autoridades de Control Independientes", 487.

los perjuicios derivados de la infracción, garantizando el principio del debido proceso" –art. 28–. En todo caso, el capítulo Xl de la LOPD ha concretado la regulación de medidas correctivas, infracciones y régimen sancionatorio, con la intervención de la autoridad de control. Ahora bien, agregamos que la ausencia –en el PLODP 2016– de las condiciones y procedimientos sancionadores pudo subsanarse, bien mediante, la modificación del proyecto; o, bien, a través de su regulación dentro del Reglamento, que se hubiese requerido para armonizar los principios y derechos vinculados con la protección de datos.

### C. Función de publicidad y registro de ficheros

Considerada como una de las principales funciones de las autoridades de protección de datos, la función de publicidad y registro de los ficheros permite garantizar el control ciudadano, sobre el tratamiento de su información y, además, sensibilizar en los responsables del tratamiento los deberes y principios que deben observarse, dentro del marco legal para la protección de datos. Son varias las razones que refieren la relevancia de esta función. Al respecto, consideramos que:

> Por una parte, el Registro de ficheros permite la publicidad de los tratamientos, lo que facilita al ciudadano el ejercicio de sus derechos; por otra, tanto el Registro de ficheros como la propia función de inscripción registral son instrumentos que ayudan a la Agencia en el cumplimiento de sus funciones de control; por último, la declaración y notificación de ficheros y tratamientos es el primer paso en el cumplimiento de la legislación y en el respeto al derecho de toda persona a controlar su información personal ya que permite al responsable tomar conciencia de que los datos personales no son suyos sino de los ciudadanos, auténticos titulares de un derecho fundamental[111].

No obstante, conviene aclarar que la obligación de inscripción o registro de los ficheros desaparece, al menos, en el contexto de la Unión Europea, por disposición del RGPD[112]. Tal como señala el RGPD, esta actividad se sustituye por

[111] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1800.

[112] Como precisa el RGPD: "La Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control. Pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales. Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos

procedimientos y mecanismos de protección razonables, que habilitan a los responsables a tomar decisiones proactivas, sobre los riesgos que se derivan del tratamiento de datos. En este orden, el PLODP 2016 estimó "crear un Registro Nacional de Bases de Datos Personales y emitir las órdenes y los actos necesarios para su administración y funcionamiento" –art. 12.7–. Conforme a este proyecto, el Registro se conformaba del "conjunto organizado de bases o bancos de datos, ficheros, archivos, en forma física o digital, de instancias públicas o privadas, que operen en el país, sujetos a tratamiento" –art. 14–. Por tanto, la función de inscripción registral precisaba que los ficheros debían "inscribirse en el Registro Nacional de Bases de Datos Personales de acuerdo con los procedimientos y criterios que la Dirección Nacional de Registro de Datos Públicos establezca para el efecto" –art. 16–.

Ahora bien, el art. 89 del PLODP 2019 ha materializado en la LOPD que la autoridad de control podrá "crear, dirigir y administrar el Registro Nacional de Protección de Datos Personales, así como coordinar las acciones necesarias con entidades del sector público y privado para su efectivo funcionamiento" –art. 76.6–. Así, en el caso de Ecuador esta función de control se cumpliría, a partir de la actividad y procedimientos que la autoridad de control implemente para el registro y, en consecuencia, la publicidad de los ficheros. Por tanto, el Registro Nacional se constituiría en una institución integrada y controlada por la autoridad de protección de datos. Así, debe tomarse en cuenta que la autoridad de control y supervisión tiende a ser "responsable de un registro público de las entidades que tratan datos personales, las cuales deben practicar notificación previa a la iniciación de las operaciones de tratamiento"[113].

Hay que considerar que, la LOPDGDD señala que "los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del Reglamento (UE)

tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial" –Considerando 89–.

[113] Cerda Silva, "Mecanismos de Control en la Protección de Datos en Europa", 221-251.

2016/679" –art. 31.1–. En este sentido, el RGPD menciona que "el responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones" –art. 31–. Precisamente, una de esas funciones es la que establece que "cada responsable y, en su caso, sus representantes llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad" –art. 30.1–. Por consiguiente, dichos registros deberán constar por escrito y en formato electrónico, de tal manera que, "el responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite" –art. 30.4–. Así, la aplicación de medidas técnicas y de mecanismos necesarios, con el apoyo de las tecnologías de la información, constituye una oportunidad para garantizar la protección de los derechos vinculados a la protección de datos. En el caso europeo, sobre este respecto, advertimos que:

> El Reglamento obliga al responsable a ser reflexivo, a llevar a cabo una valoración de la naturaleza del tratamiento y de los riesgos para los derechos de las personas y que debe realizar una evaluación de los riesgos —alto, estándar o bajo— adoptando aquellas medidas adecuadas a cada caso concreto, con un claro enfoque al riesgo —qué cosas pueden pasar para evitar que pasen—, obligando incluso al responsable a valorar el riesgo en términos de probabilidades[114].

Se trata, en definitiva, de que esta función de control de publicidad y registro de los ficheros, ya no recaiga en las autoridades de control, sino que, ahora sean las instituciones públicas y privadas las que, por medio de prácticas de autorregulación contribuyan al aseguramiento integral del derecho a la protección de datos.

### D. Función de promoción del derecho a la protección de datos

Con frecuencia suele decirse que la legislación de protección de datos incorpora una serie de normas abstractas que, a la hora de hacer efectivo este derecho fundamental, podría poner en riesgo la confianza ciudadana y la seguridad jurídica del ordenamiento legal. Por ello, la función de promoción que cumplen las autoridades de control facilita el ejercicio de los derechos de los titulares y el

[114] Troncoso, "Autoridades de Control Independientes", 465.

cumplimiento de las obligaciones, que les corresponden a los responsables. Se trata de una función preventiva, que establece un conjunto de mecanismos y actividades, las cuales aseguran la tutela y seguridad jurídica del marco legal de protección de datos. De esta manera, dentro de esta función, se enmarca la actividad "*ex ante* de control previo –*prior checking*-, que tiene un carácter básicamente preventivo y tuitivo y que es una de las justificaciones para hacer descansar la protección de datos personales en un modelo de administración y no sólo en un control jurisdiccional *ex post*"[115].

Por ejemplo, el PLODP 2016 propuso que la autoridad de control debía "promover y divulgar los derechos de las personas en relación con el tratamiento de datos personales e implementar mecanismos de difusión acerca del ejercicio y garantía del derecho constitucional de la protección de datos" –art. 12.2–. Así también "realizar campañas de concientización a la población sobre la necesidad de protección de datos personales y sensibles" –art. 12.10–. En este mismo orden, basándose en el art. 89 del PLODP 2019, la LOPD ha concretado que la autoridad de control debe "promover e incentivar el ejercicio del derecho a la protección de datos personales, así como la concientización en las personas y la comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento y uso de sus datos personales, con especial énfasis en actividades dirigidas a grupos de atención prioritaria tales como niñas, niños y adolescentes" –art. 76.16–.

Si bien, en el caso de Ecuador, nos encontramos, recientemente, ante un nuevo marco normativo o Ley General para la protección de datos; este derecho fundamental lleva reconocido en nuestra Constitución más de un decenio. En este sentido, advertimos que las actividades de promoción, divulgación y concienciación han sido, relativamente, escasas. El Ministerio de Justicia, Derechos Humanos y Cultos ha planteado, como un eje estratégico, "incrementar el cumplimiento de los derechos humanos a nivel nacional"[116]. Así también el Ministerio de

[115] Troncoso, *La Protección de Datos Personales: En busca del equilibrio*, 1809.

[116] Las actividades para concretar este eje se enmarcan en: "desarrollar mecanismos de difusión masiva de derechos humanos; implementar programas de capacitación en derechos humanos en instituciones públicas, colegios y escuelas; e, implementar una metodología para la medición de la efectividad de las políticas públicas en el cumplimiento de los derechos humanos".

Telecomunicaciones y Sociedad de la Información tiene, como un eje "incrementar el uso de las TICs en el ámbito público, privado y la sociedad en general". Instituciones, como el Consejo Nacional de la Niñez y la Adolescencia (CNNA), Consejos Cantonales y Juntas Cantonales de Protección de Derechos –orientadas a instituir un Sistema Nacional Descentralizado de Protección Integral de la Niñez y la adolescencia–, tienen como función estratégica la "aplicación e implementación de las políticas, programas, normas e instrumentación que permitan fomentar y garantizar los derechos de niños y niñas, adolescentes, jóvenes, adultos mayores y personas con discapacidad en el Ecuador" .

Éstas constituyen algunas estrategias gubernamentales sobre protección de la privacidad, de los datos personales y de la niñez y la adolescencia. No obstante, en la práctica, no se observan programas o políticas públicas concretas, que permitan equilibrar el derecho a la protección de datos, con el avance de las tecnologías de la información y comunicación. Una idea sólida que desarrolle la prevención se desprende de las actividades de difusión, asistencia y promoción, en donde la autoridad de control:

> Es responsable de la difusión de las disposiciones legales y reglamentarias aplicables al tratamiento de datos personales, ya que las más de las veces la infracción a sus preceptos encuentra su explicación en una falta de conciencia de antijuricidad del comportamiento por parte del responsable de registros o bases de datos. A tal tarea se suma la asistencia a los más diversos sectores de la comunidad (…) Además, la autoridad de control realiza acciones de promoción en la materia, por ejemplo, mediante el fomento en la aplicación de tecnologías de protección de la intimidad por las entidades que procesan datos y la adopción de códigos de conducta por los responsables de tratamiento[117].

Por ejemplo, el RGPD señala la importancia de "promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención" –art. 57.1. b)–; "promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben" –art. 57.1. d)–; y "fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos" –art. 57.1.

[117] Cerda Silva, "Mecanismos de Control en la Protección de Datos en Europa", 221-251.

n)–[118]. En este ámbito, conforme al principio de responsabilidad proactiva, un papel significativo cumple, tanto los responsables como los encargados del tratamiento. Por ello, recalcamos que:

> Esta actividad prestacional va dirigida tanto a los responsables y a los encargados de tratamiento —y a los delegados de protección de datos— que tienen que cumplir unas obligaciones en los tratamientos de datos personales y respetar unos principios y unos derechos de protección de datos, como a los ciudadanos en general que son titulares del derecho fundamental a la protección de datos personales[119].

La función de promoción del derecho a la protección de datos constituye una de las actividades, más esenciales, dentro de la función de tutela que ejercen las autoridades de control. Es imprescindible que la naturaleza de las actividades de promoción recaiga, tanto sobre los derechos que asisten a los titulares de los datos como también en las obligaciones que corresponden a los responsables y encargados del tratamiento. Además, es necesario promover en los ciudadanos una cultura de respeto de los datos personales, sobre todo en entornos digitales. En gran medida, la vigencia de este derecho depende de la "sensibilidad de los ciudadanos hacia este derecho ya que una actuación inconsciente y negligente por parte de las personas no puede ser siempre cubierta por la diligencia de las autoridades de control"[120].

A partir de esta investigación, nos hemos dedicado a estudiar varios modelos jurídicos, que sirven de referencia para construir de manera integral y equilibrada un marco jurídico, el cual responda a las necesidades que plantea el derecho a la protección de datos personales. Así, un principio básico en la legislación de protección de datos es la previsión de una autoridad de control independiente. Aspiramos que en la adecuación de la LOPD no prevalezcan los intereses políticos, sobre los derechos de los ciudadanos; y que las garantías formales y sustanciales que se atribuyen a las autoridades de control materialicen, en la práctica, un modelo

[118] Finalmente, recordemos que el art. 42.4 de los EPEI precisa que las autoridades de control deben contar con suficientes poderes de promoción y otros que resulten necesarios para garantizar el efectivo cumplimiento, así como el ejercicio y respeto del derecho a la protección de datos personales.
[119] Troncoso, "Autoridades de Control Independientes", 501.
[120] Ibíd., 503.

que propenda a tutelar la seguridad jurídica y el respeto de los derechos y libertades de los titulares de los datos de carácter personal.

## CONCLUSIONES

I. La base fundamental del derecho a la protección de datos personales nos reconduce a la necesidad de garantizar el respeto de la dignidad humana de las personas, con estricto apego a los derechos inherentes de los titulares de la información personal. Naturalmente, esta construcción se encuentra reconocida en los preceptos constitucionales de Ecuador, especialmente en su preámbulo, por cuanto, a partir del Estado constitucional de derechos y justicia se promueve una sociedad que respeta, en todas sus dimensiones, la dignidad de las personas.

II. Encontramos que son dos los principales motivos que han afianzado el desarrollo del derecho fundamental a la protección de datos personales en Ecuador. El primero está relacionado con la evolución de las tecnologías de la información y comunicación; y el segundo con los procesos de integración económica y comercial. Todo ello con el objeto de generar confianza y reforzar el derecho a la seguridad jurídica, mediante marcos normativos que aseguren la proporcionalidad de los límites al derecho a la protección de datos personales y a otras libertades fundamentales. En todo caso, a estas motivaciones se suman los efectos de la emergencia sanitaria. Uno de estos efectos, precisamente, plantea en los Estados la necesidad de preservar la privacidad y la protección de los datos personales, especialmente en lo que se refiere al tratamiento de datos sensibles.

III. La composición del derecho fundamental a la protección de datos personales se enmarca en un juego contrapuesto que atribuye, por una parte, derechos para los titulares de los datos personales; y por otra, obligaciones para los responsables de los tratamientos, en soporte material o electrónico, sobre dichos datos. En suma, este derecho fundamental engloba una serie de principios, derechos y garantías, los cuales posibilitan mantener el control de la información personal, frente a

posibles intromisiones ilegítimas en los derechos y libertades de las personas.

IV. El reconocimiento constitucional de la protección de datos personales como un derecho fundamental autónomo, el cual se garantiza mediante el *habeas data*, en los artículos 66.19 y 92 de la Constitución de Ecuador, supone considerar que, tanto en el ámbito público como privado, la base esencial para el respeto de los derechos y libertades debe ser la Constitución, por cuanto constituye una norma jurídica de aplicación directa e inmediata. Por ello, advertimos que de este reconocimiento en la Constitución nace una serie de facultades, principios y garantías tendentes a regular el tratamiento de la información personal, sea en soporte material o electrónico. Así, por ejemplo, se reconoce el derecho a acceder y decidir sobre los propios datos personales, además de incluir el ejercicio de otros derechos como el de rectificación, cancelación y oposición. Además, para la recolección, archivo, procesamiento, distribución o difusión, en suma, cualquier tratamiento de datos personales, se establece el respeto del consentimiento o autorización del titular de los datos como una garantía de legitimación o licitud, adoptando medidas de seguridad apropiadas para el caso de los datos sensibles.

V. Tanto el derecho a la protección de datos personales, como la garantía jurisdiccional del *habeas data* se estatuyen en la Constitución de Ecuador como un derecho fundamental en sí mismo, bajo el cual subyace un instituto de garantía para la protección de otros derechos y libertades. Así, como ha recalcado la Corte Constitucional de Ecuador, la protección de datos adquiere una categoría transversal o instrumental que se destina a tutelar a las personas en los casos en que el Estado o los particulares utilicen datos incorrectos, inexactos u obsoletos, teniendo en cuenta que a partir del tratamiento de datos personales se puede afectar derechos y libertades relacionados con la igualdad, intimidad o desarrollo integral de la personalidad.

VI. En el ámbito de la Comunidad Andina, salvo los casos de Argentina y Uruguay que han recibido reconocimiento europeo como países con nivel

adecuado de protección, la situación regional se presenta muy diversa a diferencia de la Unión Europea. Atendiendo los señalamientos del Comité Jurídico Interamericano de la Organización de Estados Americanos en 2015, el enfoque normativo en las Américas no ha tenido una visión uniforme o coherente. No obstante, en los últimos años, países como Ecuador han buscado concretar propuestas de regulación apegadas, no solamente a la Guía de la OEA (Principios sobre Privacidad y la Protección de Datos Personales), sino además a los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de 2017 y al Reglamento (UE) 2016/679 de la Unión Europea –en adelante RGPD–. Esto ha derivado, en el caso ecuatoriano, en la aprobación de la Ley Orgánica de Protección de Datos Personales de mayo de 2021 –en adelante LOPD–. En la búsqueda de este equilibrio y armonía regional se suman Paraguay y Bolivia que han formulado propuestas legislativas en materia de protección de datos personales.

VII. Además de los cuestionamientos ya señalados del Comité Jurídico Interamericano, advertimos la existencia de previsiones constitucionales generales en el ámbito latinoamericano, que aplicadas a casos específicos pueden desembocar en decisiones erróneas que afectarían el fundamento y la naturaleza del derecho a la protección de datos personales. Un ejemplo de esta afirmación se encontraba desarrollada en la Resolución 28/2001 del ex Tribunal Constitucional de Ecuador que enfocaba la garantía del *habeas data* como el derecho a la información. Aquello implicaba una vulneración, no solo de este derecho fundamental a la protección de datos personales, sino también del derecho a la seguridad jurídica, el cual supone la necesidad de contar con normas jurídicas claras orientadas a garantizar la confianza ciudadana. Naturalmente, de esta realidad se desprende la falta de criterios del legislador para aprobar normas que respeten la correcta técnica legislativa y que se sustenten, sobre todo, en una realidad social cierta. No obstante, dentro del Estado constitucional de derechos y justicia esta carencia estaría solventada por la plenitud constitucional que supone la

aplicación directa e inmediata de los derechos y garantías reconocidos en la Constitución de Ecuador.

VIII. El Estado constitucional de derechos y justicia reconocido en la Constitución de Ecuador establece que el máximo deber del Estado y de los particulares es promover y garantizar los derechos y libertades fundamentales. A partir del constitucionalismo contemporáneo o neoconstitucionalismo se desarrolla una nueva teoría jurídica caracterizada, principalmente: por un derecho basado más en principios que en reglas; por la relevancia del principio de ponderación; por el reconocimiento del carácter supremo de la Constitución; y, por la atribución de poderes a los jueces para la determinación de los derechos. Por tanto, con el nuevo paradigma constitucional, la Constitución deja de ser un programa político y se convierte en una norma jurídica, mediante el reconocimiento de tres bases o supuestos esenciales: a) el reconocimiento del carácter normativo superior de la Constitución; la aplicación directa de la Constitución como una norma jurídica; y, c) el reconocimiento de la jurisprudencia constitucional como una fuente primaria del derecho.

IX. Tomando en cuenta el reconocimiento del derecho fundamental a la protección de datos personales en la Constitución de Ecuador, el principio de eficacia directa supone que los derechos y garantías reconocidos en la Constitución constituyen una regla de decisión. Las decisiones de los servidores públicos, administrativos o judiciales, deben garantizar su aplicación, de manera directa e inmediata. En este marco, la falta de normativa sectorial, incluso de una Ley general, no podría significar una excusa para dejar de cumplir o declarar la justiciabilidad de un derecho. En todo caso, es preciso reconocer que uno de los pilares esenciales para que el tratamiento de la información sea legítimo y respete los derechos y libertades individuales, es la necesidad de garantizar la coherencia –seguridad jurídica– de la legislación nacional. Por tanto, bajo este paradigma, la importancia de una Ley de Protección de Datos Personales implica que el ordenamiento jurídico se respalde en normas jurídicas

claras que, enmarcadas en la Constitución, por una parte, garanticen la confianza ciudadana, y por otra, que los poderes públicos fundamenten sus actos jurídicos en nomas jurídicas previamente determinadas.

X. La jurisprudencia constitucional ecuatoriana ha desarrollado el derecho a la protección de datos personales, atendiendo a su reconocimiento constitucional. Tomando en cuenta que el contenido de los derechos se desarrollará de manera progresiva, no solamente a través de normas o políticas públicas, sino además por medio de la jurisprudencia; destacamos que son tres las sentencias de la Corte Constitucional de Ecuador que han desarrollado de mejor manera este derecho fundamental: la Resolución 19/9/2009 que precisa la esencia del principio de responsabilidad proactiva; la Resolución 1/14/2014 que reconoce la naturaleza autónoma y la garantía transversal que supone el derecho a la protección de datos personales; y, la Resolución 182/15/2015 que caracteriza las dimensiones utilitarias (informativa, aditiva, correctiva, de reserva y cancelatoria) del *habeas data*.

XI. La Reforma Constitucional de 2008 en Ecuador supuso un cambio de paradigma respecto a la garantía del derecho fundamental a la protección de datos personales. Esto es así, no solamente por las importantes resoluciones de la Corte Constitucional de Ecuador, sino además porque ha desembocado en la aprobación de una Ley general. El proyecto de reforma constitucional, afianzado en el denominado “Socialismo del Siglo XXI”, se enmarcó en la búsqueda y desarrollo de una sociedad más justa, buscando la posibilidad de una revolución en todos los niveles del Estado. Principalmente, entendemos que dos fueron los principios o nociones que consolidaron, a través del Socialismo del Siglo XXI, el reconocimiento de este derecho fundamental. Hacemos referencia, tanto a la democracia participativa como a la propuesta de derechos innovadores. En este orden, consideramos que el principio de democracia participativa contribuyó a asegurar la confianza y participación ciudadana en la propuesta constituyente; y que la noción de derechos innovadores alentó el reconocimiento de un derecho que nace, precisamente, como resultado

del avance vertiginoso de la innovación y de las tecnologías de la información y la comunicación.

XII. Con referencia a la evolución de la protección de datos personales en Ecuador, comprendemos que, en el derecho constitucional ecuatoriano, la protección de datos personales se ha desarrollado en tres etapas: primero, la protección constitucional a través del *habeas data*; segundo, la regulación de la información personal y de la intimidad con una perspectiva garantista mediante Leyes sectoriales; y tercero, el reconocimiento de un derecho fundamental a la protección de datos personales en la Constitución de 2008. En todo caso, a partir de la promulgación de la LOPD en mayo de 2021, nos encontramos atravesando ya una cuarta etapa.

XIII. En relación a la aprobación de la LOPD en mayo de 2021, varias han sido las recomendaciones expuestas por la normativa internacional para equilibrar los ordenamientos jurídicos en materia de protección de datos personales. La Organización de los Estados Americanos plantea que cada Estado miembro debe buscar la mejor manera de implementar los principios que se recomiendan en la Guía Legislativa de 2015, la cual ha merecido una actualización en abril de 2021. Así también los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de 2017 invocan la necesidad de armonizar la normativa, sobre la base de las definiciones, principios, derechos y procedimientos que componen el derecho a la protección de datos personales. En todo caso, hay que recordar que el RGPD, no solo armoniza la legislación de protección de datos personales, mediante una normativa general, sino que reconoce asimismo un margen de maniobra para una regulación más específica por medio de una normativa sectorial. De esta forma, la experiencia internacional nos demuestra que el fortalecimiento de la seguridad jurídica y, en suma, de la confianza ciudadana comprende la consolidación de un modelo mixto sustentado en la existencia de una Ley general y de una pluralidad de normas específicas, también denominadas normativa sectorial.

XIV. En el caso de Ecuador es imprescindible reconocer que tres fueron los proyectos que impulsaron la materialización de una Ley general: los proyectos de 2010, de 2016 y de 2019, todos ellos posteriores al reconocimiento constitucional de 2008. Una referencia especial debe hacerse a los principales argumentos que motivaron el archivo de la propuesta legislativa de 2010. Primero, que el proyecto no tenía la condición de Ley orgánica, a pesar de contener una normativa que desarrollaba derechos fundamentales relacionados con la protección de datos personales. Segundo, que la creación de una autoridad de control incrementaría más la burocracia, sin tomar en consideración que dicha autoridad se configura como un principio esencial de todo marco de protección de datos. Y, tercero, que la nueva normativa supondría una innecesaria expansión y repetición de acciones reconocidas en el ordenamiento jurídico nacional, olvidando con ello que el sistema de protección de datos personales exige el establecimiento de un sistema mixto.

XV. La búsqueda del equilibrio que requiere en la práctica este derecho fundamental no debe hacernos olvidar los errores cometidos por el legislador o los servidores públicos, tanto administrativos como judiciales. Este planteamiento sugiere en gran medida la necesidad de un “pacto social”, que asegure la proporcionalidad de los límites al derecho a la protección de datos personales y a otras libertades fundamentales. Por ello, entendemos que la LOPD pretende desarrollar estos presupuestos, por cuanto busca promover un marco jurídico compatible que, también en el ámbito internacional, facilite el intercambio y al mismo tiempo respete y proteja los derechos humanos.

XVI. El objeto y finalidad de la LOPD aprobada en mayo de 2021 supone el desarrollo del derecho de libertad reconocido en el artículo 66.19 de la Constitución de Ecuador, estableciendo que su objeto es garantizar el ejercicio del derecho fundamental a la protección de datos personales, lo cual incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. En todo caso, hay que

criticar, por una parte, que el legislador haya olvidado reconocer la protección de otros derechos y libertades, que puedan estar relacionados con este derecho fundamental; y, por otra, además, que no haya incluido en su objeto una referencia expresa a la importancia de garantizar la libre circulación de los datos personales, como se encuentra en el marco normativo europeo. En este sentido, el legislador ecuatoriano ha desconociendo la categoría transversal que comprende la protección de este derecho fundamental y, además, ha limitado la libre circulación de los datos personales.

XVII. En el ámbito de aplicación material y territorial, la normativa de protección de datos personales de Ecuador, recientemente aprobada, regula adecuadamente los tratamientos de datos personales, sean o no automatizados y, además, establece su cumplimiento para responsables y encargados del tratamiento domiciliados, tanto dentro del territorio nacional como fuera de este. En este marco, una especial referencia merecen las excepciones al ámbito de aplicación relativas a los datos de personas jurídicas y a los datos anonimizados. Si bien el art. 2. g) de la LOPD, estima que la Ley no será aplicable a “los datos que identifican o hacen identificable a personas jurídicas”, dicha norma, al mismo tiempo, precisa que serán susceptibles de tratamiento los datos personales de las personas asociadas o de sus representantes legales. Hay que subrayar que esta excepción respeta la Resolución 1/14/2014 de la Corte Constitucional de Ecuador al establecer que el derecho a la protección de datos personales no se limita a la calidad de las personas jurídicas como titulares del mismo. Sin duda, en este caso reconocemos que el legislador ha respetado los criterios sentados por la jurisprudencia constitucional y, en todo caso, ha materializado la garantía del principio de juridicidad, por el cual los tratamientos de datos personales se regulan también por medio de la jurisprudencia que resulte aplicable. En cuanto a la excepción de los tratamientos de datos anonimizados, si bien no entran en el ámbito de aplicación de la normativa de protección de datos personales, pueden existir casos en los que una información disociada puede convertirse en un dato de una persona identificable. Por ello, nos parece importante que

la LOPD prescriba que tan pronto los datos dejen de ser anónimos, su tratamiento estará sujeto al cumplimiento de las obligaciones de la normativa de protección de datos personales.

XVIII. La LOPD incorpora acertadamente importantes definiciones, las cuales pretenden promover en la sociedad, especialmente, en los poderes públicos el respeto y garantía de la seguridad jurídica, como base para la confianza ciudadana y coherencia del marco jurídico de protección de datos personales. Desde esta perspectiva, hay que destacar la descripción de conceptos relacionados con: autoridad de protección de datos personales; anonimización y seudonimización; base de datos o ficheros; consentimiento; datos biométricos, genéticos, personales, crediticios, relativos a la salud y datos sensibles; delegado de protección de datos; responsable y encargado del tratamiento; entidades de certificación y sellos de protección.

XIX. El consentimiento se encuentra correctamente definido en la LOPD como una manifestación de la voluntad libre, específica, informada e inequívoca del titular de este derecho fundamental. Así, transponiendo los preceptos constitucionales, dicha voluntad requiere de la autorización del titular de los datos personales. Por tanto, entendemos que el consentimiento se constituye como una garantía esencial de legitimación de los tratamientos de la información personal. Ahora bien, teniendo en cuenta la normativa internacional, hay que cuestionar la ausencia en la LOPD de la obligación de que se demuestre que dicho consentimiento fue obtenido, ya sea a través de una declaración o una acción afirmativa clara. En todo caso, a la luz del RGPD, la Resolución 2064/14/2021 de la Corte Constitucional de Ecuador ha destacado la importancia de respetar estas dos formas de obtener el consentimiento. De esta forma, para asegurar que el consentimiento haya sido obtenido por medios legítimos y, en suma, afianzar la transparencia de los tratamientos es importante subrayar la necesidad de una propuesta de *lege ferenda* en este sentido.

XX. La LOPD reconoce acertadamente que ciertos datos personales constituyen categorías especiales, los cuales merecen medidas de protección apropiadas atendiendo los preceptos constitucionales del *habeas data*. Esta exigencia se deriva de la facultad de controlar que su conocimiento, divulgación y tratamiento por terceros afecte o lesione, en mayor medida, derechos vinculados con la intimidad, dignidad y honor de las personas. Con referencia a este aspecto, subrayamos que la introducción de estos tipos específicos de datos proviene del mandato constitucional previsto en el art. 11.2 de la Constitución de Ecuador, por el cual se reconoce la igualdad y la prohibición de discriminación. Por otra parte, si bien la protección de los datos genéticos también está reconocida en el *habeas data*, hay que reconocer que la LOPD ha introducido apropiadamente como una novedad, la protección y definición de los datos biométricos.

XXI. Si bien la garantía de *habeas data* reconoce las facultades de control de los datos personales por medio del ejercicio de los derechos de acceso, rectificación, cancelación y oposición; la LOPD ha introducido otros derechos distintos de los derechos ARCO que ya se encuentran recogidos en la normativa internacional. Nos referimos a los derechos de portabilidad; limitación del tratamiento y sobre decisiones individuales automatizadas, incorporando las novedades del RGPD. Sobre el derecho de rectificación, hay que cuestionar que la LOPD no determine que la solicitud de rectificación pueda hacerse por medio de una declaración adicional, lo cual implica un nuevo derecho del titular de los datos. Por otra parte, en relación con el derecho de supresión expresado como derecho al olvido en el RGPD, este derecho ha sido una de las principales innovaciones de la normativa internacional, que se encontraba incluida en la propuesta legislativa de 2019. No obstante, el legislador finalmente desestimó su reconocimiento en la normativa de protección de datos personales aprobada en mayo de 2021, algo que debe criticarse. Finalmente, en relación a la limitación al tratamiento advertimos que el legislador ha considerado que esta limitación al tratamiento se califica como un derecho a la suspensión.

XXII. Hay que criticar que no quedan claras las obligaciones del encargado del tratamiento en la LOPD. Tomando en cuenta que el responsable del tratamiento determina los fines y medios del tratamiento y que el encargado trata datos personales por cuenta del responsable; no parece apropiado que la normativa de protección de datos personales recientemente aprobada no distinga adecuadamente las diferentes obligaciones del responsable y del encargado de tratamiento. En todo caso, celebramos la incorporación de nuevas obligaciones relacionadas con las evaluaciones de impacto; la privacidad desde el diseño y por defecto; y, la obligación de contar con un delegado de protección de datos. Todo esto, no solamente supone cumplir con la legislación, sino vigilar y demostrar permanentemente que ésta se cumpla. Por ello, atendiendo al principio de responsabilidad proactiva, el responsable debe coadyuvar a este objetivo, mediante la adopción de medidas apropiadas, que garanticen y acrediten el cumplimiento de los principios de la protección de datos personales.

XXIII. El reconocimiento de principios que desarrollen la tutela del derecho fundamental a la protección de datos personales garantiza que el tratamiento de la información personal cumpla con el respeto de los derechos y libertades de las personas. Por ello, hay que celebrar que la LOPD describa importantes principios como: juridicidad; lealtad; transparencia; finalidad; pertinencia y minimización de datos; proporcionalidad; confidencialidad; calidad y exactitud; conservación; seguridad; responsabilidad proactiva y demostrada; aplicación favorable al titular; e independencia del control. En este marco, algunos de ellos nacen del plexo de garantías reconocido en el *habeas data*, que al final nos reconduce a respetar las condiciones por las cuales el tratamiento se considera como lícito, proporcional, pertinente y transparente. Naturalmente, el principio de responsabilidad proactiva o demostrada compromete que el responsable, no solamente debe cumplir con todos estos principios, sino que además tendrá que adoptar medidas o mecanismos diligentes tendentes a demostrar su cumplimiento.

XXIV. La protección de datos personales de los menores merece siempre una especial atención en Ecuador, teniendo en cuenta nuestra realidad social donde muchos menores se encuentran muchas horas abandonados y privados de un acompañamiento familiar adecuado. Redes sociales e Internet representan un gran avance en los procesos de desarrollo de las sociedades modernas. No obstante, si bien los objetivos del desarrollo tecnológico se orientan a eliminar la brecha y analfabetismo digital, la falta de concienciación sobre los peligros que supone el acceso a medios informáticos constituye una de las principales problemáticas, sobre todo en lo concerniente al respeto del derecho a la protección de datos personales y a la intimidad informática. Por ello, en la actualidad el respeto del derecho a la protección datos personales y la privacidad de los menores en la red tiene una especial importancia. En el caso de la niñez y la adolescencia, el instituto de garantía que comprende la protección de la información personal exige la adopción de mecanismos especiales de tutela, los cuales se derivan, tanto del principio de corresponsabilidad como del interés superior del menor. En este plano, hay que subrayar la relevancia que tendrá el desarrollo del derecho a la educación digital previsto en la LOPD.

XXV. El establecimiento de una autoridad de protección de datos personales en Ecuador, recogida en la normativa recientemente aprobada, asegura una estructura jurídica integral, la cual proporciona a los ciudadanos herramientas y mecanismos transversales de protección de sus derechos y libertades fundamentales. Esta autoridad es un pilar y un principio esencial de nuestro ordenamiento de protección de datos personales pues, institucionalmente, se encarga de la vigilancia, tutela y el respeto de los derechos que se derivan de este derecho fundamental. Además, a través del establecimiento de una autoridad de control se posibilita una aplicación más flexible y referida al caso concreto en el cumplimiento de la legislación de protección de datos personales. Como expresa la Guía legislativa de la OEA es fundamental establecer órganos de supervisión que sean suficientemente independientes. Por ello, en este ámbito, es importante subrayar la carencia en la normativa aprobada de

las garantías sustanciales y formales de independencia debidamente acreditadas. La LOPD contiene previsiones muy generales, tan solo sobre la forma y requisitos para el nombramiento e inamovilidad del titular de la autoridad de control. De esta forma, si la intención de la legislación de protección de datos personales es concretar un nivel adecuado de protección y un marco jurídico compatible en el ámbito internacional, es necesario subrayar la conveniencia de reformar este apartado de la LOPD para que no prevalezcan los intereses políticos sobre los derechos de los ciudadanos. Es esencial la atribución a las autoridades de control de garantías formales y sustanciales de independencia para que se establezca en la practica un modelo que propenda a tutelar la seguridad jurídica y el respeto de los derechos y libertades de los titulares de los datos personales.

## BIBLIOGRAFÍA


Adsuara Varela, Borja. “El consentimiento”, en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*. Madrid, Reus, 2016.

Adsuara Varela, Borja. “El ciudadano frente al Reglamento”. en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Acedo Ángel y Platero Alejandro, “La privacidad de los niños y adolescentes en las redes sociales: Referencia especial al régimen normativo europeo y español, con algunas consideraciones sobre el chileno”, *Revista Chilena de Derecho y Tecnología,* No. 5. 2016. 63-94.

Agencia de los Derechos Fundamentales de la Unión Europea (Consejo de Europa), Manual de legislación europea en materia de la protección de datos. Luxemburgo: Oficina de Publicaciones de la Unión Europea, 2018.

Agencia Española de Protección de Datos. Infografía sobre Protección de Datos y Prevención de Delitos. Disponible en https://tinyurl.com/yy2rauon.

Álvarez Rigaudias, Cecilia. “El tratamiento y sus responsables”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Álvarez Valenzuela, Daniel. “Acceso a la Información Pública y Protección de Datos Personales. ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos?”, *Revista de Derecho: Universidad Católica del Norte*, No. 1. 2016.

Amnistía Internacional, Derechos Humanos para la Dignidad Humana. Madrid: Editorial Amnistía Internacional, 2005.

Aparicio Salom, Javier. “Derechos del interesado (Arts. 12-19)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Aparicio Salom, Javier. “Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Aperribai Ulacia, Ana y Intxaurtieta Madariaga, Román. “Consideraciones de la Agencia Vasca de Protección de Datos”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Arenas Ramiro, Mónica. “La protección de datos personales en los países de la Unión Europea”, *Revista Jurídica de Castilla y León*, Nro. 16. 2008. 113-168.

Arenas Ramiro, Mónica. “El valor de la información personal: Protección de datos personales y la sociedad del espectáculo”, Anuario Facultad de Derecho – Universidad de Alcalá, Nro. 2. 2009. 275-300.

Arenas Ramiro, Mónica. “*Unforgettable*: A propósito de la STJUE de 13 de mayo de 2014. Caso Costeja (*Google* Vs. AEPD)”, *Revista Teoría y Realidad Constitucional*, Nro. 34. 2014. 537-558.

Arenas Ramiro, Mónica. “Partidos políticos, Opiniones políticas e Internet: La lesión del derecho a la Protección de Datos Personales”, *UNED: Revista Teoría y Realidad Constitucional, No.* 44. 2019. 341-372.

Arias Pou, María. “Definiciones a efectos del Reglamento General de Protección de Datos”, en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*. Madrid, Reus, 2016.

Ávila, Luis Fernando. *Política, Justicia y Constitución*. Quito-Ecuador: Corte Constitucional para el Período de Transición, 2012.

Ávila Santamaría, Ramiro. *Los derechos y sus garantías. Ensayos críticos.* Quito-Ecuador: Corte Constitucional para el Período de Transición. 2012.

Ávila Santamaría, Ramiro. *El Neoconstitucionalismo andino.* Quito-Ecuador, Universidad Andina Simón Bolívar, 2016.

Bajo, Juan Carlos. “Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el *compliance*”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Bauzá, Marcelo. “Derechos Fundamentales”, en *Privacidad y Tecnología en equilibrio*. Uruguay: Unidad Reguladora y de Control de Datos Personales, 2012.

Bazán, Víctor. “El habeas data y el derecho a la autodeterminación informativa en perspectiva de Derecho Comparado”, *Estudios Constitucionales: Revista del Centro de Estudios Constitucionales*, No. 2. 2005.

Bidart Campos, Germán. *Teoría general de los derechos humanos*. México: Instituto de Investigaciones Jurídicas, 1993.

Blanco Antón, María José. “Cooperación con la autoridad de control (Art. 31)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Blanco Antón, María José. “Autoridades de control independiente (Arts. 55-59)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Bobbio, Norberto. *El tiempo de los derechos humanos.* Madrid, Editorial Sistema. Fundación Sistema, 1991.

Borón, Atilio “El socialismo del siglo XXI: Notas para su discusión”, en: *Los Nuevos Retos de América Latina: Socialismo y Sumak Kawsay*. Quito-Ecuador, SENPLADES, 2010.

Brian Nougreres, Ana. “El sistema uruguayo de protección de datos personales y su posicionamiento global”, *Revista Latinoamericana de Protección de Datos Personales*, No. 5. 2018. Disponible en: https://tinyurl.com/uj7kyf2

Cano-Nava, Martha Olivia. “Modelo epistemológico de la teoría tridimensional del derecho”, *Revista de Ciencias Sociales: Convergencia*, No. 57. 2011.

Carbonell, Miguel. “Prologo”, en Ramiro Ávila Santamaría, *Neoconstitucionalismo y Sociedad.* Quito-Ecuador: Ministerio de Justicia y Derechos Humanos, 2008.

Carrasco Salayero, Ignacio. “Cloud Computing”, en José López Calvo (coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*. Madrid. Wolters Kluwer. 2018.

Casanova Asencio, Andrea. “Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias”, *Indret: Revista para el análisis del Derecho, No.* 1. 2019. 1-31.

Castillo Córdova, Luis. *Hábeas Corpus, Amparo y Hábeas data.* Lima-Perú: ARA Editores, 2003.

Cerda Silva, Alberto. “El nivel adecuado de protección para las transferencias internacionales de datos personales desde la Unión Europea”, *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, No. 1. 2011.

Cerda Silva, Alberto. “Mecanismos de Control en la Protección de Datos en Europa”, *Revista Ius et Praxis*, No. 2. 2006.

Comanducci, Paolo. “Formas de Neoconstitucionalismo: un análisis metateórico”, en Miguel Carbonell (coord.), *Neoconstitucionalismo.* Madrid, Editorial Trotta, 2003.

Corte Suprema de Justicia, “Protección de Datos Personales”, en Víctor Núñez (coord.). Asunción – Paraguay: División de Investigación, Legislación y Publicaciones – Centro Internacional de Estudios Judiciales, 2010.

Costa Hernandis, Raúl. “Responsabilidad del responsable del tratamiento (Art. 24)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Chivi Vargas, Idón. *Nueva Constitución Política del Estado: Conceptos fundamentales para su desarrollo normativo*. La Paz – Bolivia: Vicepresidencia del Estado Plurinacional, 2010.

Davara, Miguel. *Anuario de Derecho de las Tecnologías de la Información y las Telecomunicaciones (TIC) 2002. Trabajos doctrinales especializados, boletines de actualidad, reseñas de interés jurídico, glosario de términos, preguntas más frecuentes y otras informaciones de interés*. Madrid: Fundación Airtel, 2005.

Davara Fernández, Laura. *Menores en Internet y Redes Sociales: Derecho Aplicable y Deberes de los Padres y Centros Educativos. Breve referencia al fenómeno Pokémon Go*. Madrid. 2017.

De la Serna Bilbao, María Nieves. “Las tecnologías de la información; derecho a la privacidad, tratamiento de datos y tercera edad”, *Oñati Socio-Legal Series*, Nro. 8 (2011). ISSN 2079-5971.

De la Serna Bilbao, María Nieves “La protección de datos en el sector farmacéutico”, en Jordi Faus Santasusana y José Vida Fernández (coord.), *Tratado de Derecho Farmacéutico. Estudio del régimen jurídico de los medicamentos*. España. Aranzadi. 2017.

Dieterich Steffa, Heinz. “El Socialismo del Siglo XXl”, Recuperado de: http://noblogs.org/oldgal/737/SocialismoXXI.pdf.

Doneda, Danilo. “A proteção dos dados pessoais como direito fundamental, *Revista Espaço Jurídico*, No.2. 2011.

Eguiguren Praeli, Francisco. “El derecho a la protección de los datos personales. Algunos temas relevantes de su regulación en el Perú”, *THĒMIS-Revista de Derecho* No. 67. 2015.

Figari, Héctor y Quiroz, María del Carmen. “La protección de datos personales: Una herramienta para promover la inversión”. *THĒMIS-Revista de Derecho* No. 61. 2012.

Frosini, Tommaso Edoardo. “Nuevas tecnologías y constitucionalismo”, *Revista Derecho del Estado*, No. 15. 2003.

Galvis Cano, Lucero. “Protección de datos en Colombia, avances y retos”, *Revista Lebret de la Universidad Santo Tomás*, No. 4. 2012. 195-214.

García González, Aristeo. “La protección de datos personales: Derecho fundamental del siglo XXl. Un estudio comparado”, *Boletín Mexicano de Derecho Comparado*, No. 120. 2007.

García Mahamut, Rosario. “Partidos políticos y derecho a la protección de datos en campaña electoral: Tensiones y conflictos en el ordenamiento español”, *UNED: Revista Teoría y Realidad Constitucional,* Nro*.* 35. 2015. 309-338.

García Mexia, Pablo y Perete Ramírez, Carmen. “Internet y el Reglamento General de Protección de Datos”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Gil Rendón, Raymundo. *Derecho procesal constitucional.* México: Fundap, 2004.

Gómez Corona, Esperanza. “Derecho a la propia imagen, nuevas tecnologías e Internet”, en Lorenzo Cotino Hueso (Ed.), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*. Valencia. Universidad de Valencia. 2011. 444-466.

González Ubierna, Ignacio. “Seguridad del tratamiento (Art. 32)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Gozaíni, Osvaldo. *Derecho procesal constitucional: Hábeas Data-Protección de datos personales.* Buenos Aires: Rubinzal-Culzoni Editores, 2001.

Gregorio, Carlos. “Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina”, en Raúl Márquez Romero (coord.), *Transparentar al Estado: La experiencia mexicana de acceso a la información.* México: Instituto de Investigaciones Jurídicas, 2005.

Grijalva, Agustín. *Constitucionalismo en Ecuador*. Quito-Ecuador: Corte Constitucional para el Período de Transición, 2012.

Guastini, Riccardo. “La ‘constitucionalización’ del ordenamiento jurídico: el caso italiano”, en Miguel Carbonell (coord.), *Neoconstitucionalismo.* Madrid: Editorial Trotta, 2003.

Herrán, Ana Isabel. *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*. Madrid: Dykinson, 2002.

Hiram, Víctor Hugo. “Derecho a la protección de datos personales. Su diseño constitucional”, *Revista de Estudios en Derecho a la Información*, No. 2. 2016.

Jijena Leiva, Renato. “Tratamiento de Datos Personales en el Estado y acceso a la información pública”, *Revista Chilena de Derecho y Tecnología*, No. 2. 2013.

Kemp, Simon. *Global Digital Report in 2018*. Disponible en: https://wearesocial.com/blog/2018/01/global-digital-report-2018

Kemp, Simon. *Global Digital Report in 2019*. Disponible en: https://wearesocial.com/blog/2019/04/the-state-of-digital-in-april-2019-all-the-numbers-you-need-to-know.

Ledesma Uribe, José. “En torno a la teoría tridimensional del derecho de Miguel Reale”, *Anuario del Departamento de Derecho de la Universidad Iberoamericana*, No. 33. 2003.

López Calvo, José. “Un Reglamento poliédrico que necesita un acercamiento poliédrico”, en José López Calvo (coord.), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*. Madrid. Wolters Kluwer. 2018.

López Eduardo y Mora, Juan. “Un análisis de la estructura institucional de protección de datos en España: Un análisis jurídico y económico de la incidencia de las autoridades de control españolasen la garantía del derecho fundamental de autodeterminación informativa”, *Indret – Revista para el análisis del derecho*, No. 2. 2009.

López Sánchez, Rogelio y Leal Espinoza, José. *El derecho a la información y datos personales en México: una visión comparada con el sistema interamericano y europeo de derechos humanos*. Madrid: Dykinson, 2018.

Losing, Norbert. “La justicia constitucional en Paraguay y Uruguay”, en *Anuario de Derecho Constitucional Latinoamericano*. Montevideo-Uruguay: Konrad-Adenauer-Stiftung, 2002.

Lucas Murillo de la Cueva, Pablo. “El derecho a la autodeterminación informativa y la protección de datos personales”, *Eusko Ikaskuntza. Miramar Jauregia. Miraconcha*, Nro. 20. 2008. 43-58.

Lucas Murillo de la Cueva, Pablo. “La protección de los datos de carácter personal en el horizonte de 2010”, *Anuario Facultad de Derecho – Universidad de Alcalá* Navarra, Nro. 2. 2009.

Lucas Murillo de la Cueva, Pablo y Piñar Mañas, José Luis. El *derecho a la autodeterminación informativa*. Madrid-México: Fontamara S.A, 2011.

Maqueo Ramírez, María., Moreno, Jimena y Recio Gayo, Miguel. “Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario”, *Revista de Derecho (Valdivia)*, *No*. 1. 2017.

Martos, Natalia. “Principios (Arts. 6-11)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Milanes, Valeria. “Desafíos en el debate de la protección de datos para Latinoamérica”, *Revista Transparencia y Sociedad – Consejo para la Transparencia de Chile*, Nro. 5. 2017.

Miralles López, Ramón. “Derecho de portabilidad (Art. 20)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Miralles López, Ramón. “Protección de datos desde el diseño y por defecto (Art. 25)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Miralles López, Ramón. “Evaluación de impacto relativa a la protección de datos y consulta previa (Arts. 35 y 36)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Montaña, Juan y Pazmiño, Patricio. “Algunas consideraciones acerca del nuevo modelo constitucional ecuatoriano”, en Jorge Benavides Ordóñez y Jhoel Escudero Soliz (coord.), *Manual de justicia constitucional ecuatoriana,* Quito-Ecuador: Centro de Estudios y Difusión del Derecho Constitucional, 2013.

Muñoz Ontier, Joaquín. “Disposiciones Generales (Arts. 1-5)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Muroi Bas, Xavier. “La Agencia de Protección de Datos”, *Revista Administración Pública*, No. 147. 1998.

Nikken, Pedro. “Sobre el concepto de Derechos Humanos”, en Instituto Interamericano de Derechos Humanos, *Seminario de Derechos Humanos.* San José – Costa Rica: IIDH, 1997.

Ornellas Núñez, Lina y López Ayllón, Sergio. “La recepción del derecho a la protección de datos en México: Breve descripción de su origen y status legislativo”, en Instituto Federal de Acceso a la Información Pública, “*Compendio de lecturas y legislación: Protección de Datos Personales”*, México: Instituto Federal de Acceso a la Información Pública, 2010.

Oró, Ramon. *La protección de datos*. Barcelona: Oberta UOC, 2015.

Ortega Giménez, Alfonso. “La desprotección internacional del titular del de derecho a la protección de datos de carácter personal”, *Revista Castellano-Manchega de Ciencias Sociales*, Nro. 19. 2015. 37-56.

Oryazabal, Mario. “El Derecho a la Intimidad y el tratamiento de datos personales en el Derecho Internacional Privado Argentino”, *Revista de la Facultad de Derecho de la Universidad Nacional de Buenos Aires*, No. 83. 2007.

Otero, Paula “Sharenting… ¿la vida de los niños debe ser compartida en las redes sociales?”, *Arch Argent Pediatr.* 2017.

Palazzi, Pablo. “Avances en la protección de datos personales en América Latina”, *Revista Latinoamericana de Protección de Datos Personales*, No. 3. 2011.

Palazzi, Pablo. “Periodismo de datos y datos personales: algunas reflexiones sobre la aplicación de la ley de protección de datos personales a la prensa en la Argentina.”, *Revista Latinoamericana de Protección de Datos Personales*, No. 3. 2012.

Palazzi, Pablo. “El reconocimiento en Europa del derecho al olvido en Internet”, *Revista Jurídica: La Justicia Uruguaya,* No. 150. 2014. ISSN 0797-2695. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=5743527

Patiño, Ricardo. “Diferencias entre el socialismo del siglo XX y el socialismo del siglo XXI. La democracia participativa y el nuevo sujeto revolucionario”; en: *Los Nuevos Retos de América Latina: Socialismo y Sumak Kawsay*. Quito-Ecuador, SENPLADES, 2010.

Pérez Bes, Francisco. “La obligación de notificar una violación de seguridad de datos personales”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Pérez Gómez, José María. “Especialidades en el sector sanitario”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Pérez Luño, Antonio. *La tercera generación de derechos humanos*. Navarra: Aranzadi, 2006.

Pérez Luño, Antonio. *Manual de Informática y Derecho.* Madrid: Editorial Ariel S.A, 1996.

Pérez Luño, Antonio. *Derechos Humanos, Estado de Derecho y Constitución*. Madrid: Tecnos, 2010.

Pérez-Luño Robledo, Enrique, *El procedimiento de Habeas Data: El derecho procesal ante las nuevas tecnologías*. Madrid: Editorial Dykinson S.L, 2017.

Pinto Ferreira, Luiz. “Os instrumentos processuais protetores dos direitos no Brasil”, en Domingo García Belaunde (coord.), *La jurisdicción constitucional en Iberoamérica*. Madrid: Dykinson, 1997.

Piñar Mañas, José Luis. “Introducción. Hacia un nuevo modelo europeo de protección de datos”, en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad.* Madrid, Reus, 2016.

Piñar Mañas, José Luis. “Objeto del Reglamento”, en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad.* Madrid, Reus, 2016.

Prensky, Marc. “Nativos e Inmigrantes Digitales”, *Cuadernos SEK 2.0 – Institución Educativa SEK,* Depósito legal: M-24433. 2010.

Procuraduría de los Derechos Humanos de Guatemala, Informe Anual Circunstanciado: Situación de los Derechos Humanos y Memoria de Labores 2015, p. 380. Recuperado de: http://www.pdh.org.gt/archivos/descargas/Biblioteca/Informes%20Anuales/iac_2015._f0.pdf.

Puccinelli, Oscar. “Tipos y subtipos de hábeas data en América Latina”, *Editorial Astrea*, No. 4 (2004), 1-20 Consultado en Base de Datos: Vlex.com: ‹https://app.vlex.com/#WW/vid/26542396/graphical_version›.

Puccinelli, Oscar. “Apuntes sobre el derecho, la acción y el proceso de hábeas data a dos décadas de su creación”, en Eduardo Ferrer y Arturo Zaldívar (coord.), *La Ciencia del Derecho Procesal Constitucional: Procesos Constitucionales de la Libertad.* México, Instituto de Investigaciones Jurídicas, 2008.

Puccinelli, Oscar. *El Habeas Data en Indoiberoamérica*. Santa Fe de Bogotá-Colombia: Editorial Temis S.A, 1999.

Puccinelli, Oscar. "Un proyecto de reforma a la ley 25.326 que está a la altura de las leyes más avanzadas del mundo", *Revista Latinoamericana de Protección de Datos Personales*, No. 4. 2017. Disponible en: https://tinyurl.com/v3mgvrs

Puyol Montero, Javier. "Los principios del Derecho a la Protección de Datos", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad.* Madrid, Reus, 2016.

Puyol Montero, Javier. "El Reglamento General de Protección de Datos, y la *Pymes*", en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Rallo Lombarte, Artemi. "Hacia un nuevo sistema europeo de protección de datos: Las claves de la reforma*", UNED: Revista de Derecho Político*, Nro. 85. 2012. 13-56.

Rallo Lombarte, Artemi. "De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)", *UNED: Revista de Derecho Político*, Nro. 100. 2017. 639-669.

Rallo Lombarte, Artemi. "El nuevo derecho a la protección de datos", *Revista Española de Derecho Constitucional*, No. 116. 2019. 45-74.

Reale, Miguel. *Teoría Tridimensional del Derecho.* Madrid: Editorial Tecnos, 1997.

Recio Gayo, Miguel. *Protección de datos personales e Innovación: ¿(In) compatibles?* Madrid: Reus, 2016.

Remolina, Nelson. *Derecho de Internet & Telecomunicaciones.* Bogotá: Legis, 2003.

Remolina, Nelson. "Data Protection: Riesgos y Desarrollos (Énfasis en el caso colombiano)", *Revista Chilena de Derecho Informático*, No. 7. 2005.

Remolina, Nelson. "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?", *International Law: Revista Colombiana de Derecho Internacional*, No. 16. 2010.

Remolina, Nelson. "¿Derecho al olvido en el ciberespacio? Principios internacionales y reflexiones sobre las regulaciones latinoamericanas", en Agustina Del Campo (coord.), *Hacia una Internet libre de censura II: Perspectivas en América Latina*. Buenos Aires. Universidad de Palermo. 2017.

Remolina, Nelson y Álvarez Zuluaga, Luisa, *Guía GECTI para la implementación del principio de responsabilidad demostrada –accountability- en las transferencias internacionales de datos personales. Recomendaciones para los países latinoamericanos.* Bogotá. Facultad de Derecho – GECTI. 2018.

Reyes Kahansky, Carolina. "El deber de notificar y el derecho a la no inculpación en la protección de datos personales", *UNED: Revista de Derecho,* Nro. 24. 2019. 281-318.

Ripol Carulla, Santiago. "Aplicación territorial del Reglamento", en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*. Madrid, Reus, 2016.

Rivera Santivañez, José. *Jurisdicción Constitucional: Procesos constitucionales en Bolivia.* Cochabamba – Bolivia, 2011.

Rodríguez Marcano, Eligio. “El derecho fundamental a la protección de datos de carácter personal en Venezuela y su recorrido y reconocimiento desde la Sala Constitucional del Tribunal Supremo de Justicia de Venezuela”, *Revista Latinoamericana de Protección de Datos Personales*, No. 1. 2015.

Rodríguez Pérez, María. “Tridimensionalismo jurídico y protección de datos personales frente a su tratamiento automatizado”, *Saberes: Revista de estudios jurídicos, económicos y sociales*, Vol. 1. 2003.

Rodríguez, Paulo., Castaldi, Thays y Bruno, Giovanna. “A Nova Lei Geral de Proteção de Dados no Brasil”, *Revista Latinoamericana de Protección de Datos Personales*, No. 5. 2018. Disponible en: https://tinyurl.com/yxxq3bmv.

Rojas Bejarano, Marcela. “Evolución del derecho de protección de datos personales en Colombia respecto a estándares internacionales”, *Revista Novum Jus*, No. 1. 2014. ISSN 1692-6013, 107-139.

Roth Deubel, André-Noel. “Políticas Públicas: Formulación, Implementación y Evaluación”, *Ediciones Aurora.* 2002.

Sagués, Néstor Pedro. “El *Habeas Data*: su desarrollo constitucional”, en *V Congreso Iberoamericano de derecho Constitucional*, México: Instituto de Investigaciones Jurídicas, 1998.

Sánchez Ors, Carme. “El Delegado de Protección de Datos. Guardián de la Privacidad (Arts. 37, 38 y 39)”, en José López Calvo (coord.), El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos. Madrid. Wolters Kluwer. 2018.

Serna, Pedro. “Derechos fundamentales: el mito de los conflictos. Reflexiones teóricas a partir de un supuesto jurisprudencial sobre intimidad e información”, *Humana Iura: suplemento de derechos humanos,* No. 4.1994.

Serrano Pérez, María Mercedes. “El derecho fundamental a la protección de datos. Su contenido esencial”, *Anuario multidisciplinar para la modernización de las Administraciones Públicas*, Nro. 1. 2005.

Serrano Pérez, María Mercedes. “El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del Reglamento General de Protección de Datos y de la Ley de Protección de Datos Personales y garantía de los derechos”, *Estudios de Deusto. Revista de la Universidad de Deusto*, Nro. 2. 2020.

Tovar, Luis Freddyur. “Positivación y Protección de los Derechos Humanos: Aproximación Colombiana”, *Revista Criterio Jurídico de la Pontificia Universidad Javeriana*, No. 2. 2008.

Troncoso, Antonio. *La Protección de Datos Personales: En busca del equilibrio*. Valencia: Tirant lo Blanch, 2010.

Troncoso, Antonio. “Hacia un nuevo marco jurídico europeo de la protección de datos personales”, *Revista Española de Derecho Europeo*, No. 43. 2012.

Troncoso, Antonio. “El desarrollo de la protección de datos personales en Iberoamérica desde una perspectiva comparada y el reequilibrio en los modelos de protección de datos a nivel internacional”, *Revista Latinoamericana de Protección de Datos Personales*, No. 5. 2012. Disponible en: https://tinyurl.com/rvtguwp

Troncoso, Antonio. “Autoridades de Control Independientes”, en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*. Madrid, Reus, 2016.

Troncoso, Antonio. “La protección de datos personales como limite al acceso a la información pública en la Ley 19/2013, de 9 de diciembre. Comentario al artículo 15 <Protección de datos personales>”, en Antonio Troncoso (Dir.), *Comentario a la Ley de transparencia, Acceso a la Información Pública y Buen Gobierno.* Navarra, Aranzadi. 2017.

Troncoso, Antonio. “Del principio de seguridad de los al derecho a la seguridad digital”, *Revista Economía Industrial*, Nro. 410. 2018. 127-151.

Troncoso, Antonio. “Investigación, salud pública y asistencia sanitaria en el Reglamento General de Protección de Datos de la Unión Europea y en la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales”, *Revista de Derecho y Genoma Humano. Genética, Biotecnología y Medicina Avanzada*, No. 49, 2018.

Troncoso, Antonio. “Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de Derechos Digitales”, *Derecom*, Nro. 26. 2019. 131-140.

Trujillo, Julio Cesar. “Las Garantías Jurisdiccionales”, Recuperado de: Base de datos: Vlex.com.ec: https://app.vlex.com/#WW/vid/515951146/graphical_version.

Unicef (Fondo de las Naciones Unidas para la Infancia), “*El Estado Mundial de la Infancia 2017: Niños en un mundo digital*”. Disponible en: https://www.unicef.org/spanish/publications/files/SOWC_2017_SP.pdf

Unidad Reguladora y de Control de Datos Personales. “Memoria Anual de la Unidad Reguladora y de Control de Datos Personales”, 2015. Disponible de: https://tinyurl.com/ukrckb6

Uriarte Landa, Iñaki. “Ámbito de aplicación material”, en José Luis Piñar Mañas (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*. Madrid, Reus, 2016.

Villacrés, José Fernando. “La aplicación directa de la Constitución frente al prevaricato en Ecuador”, en Jorge Benavides Ordóñez y Jhoel Escudero Soliz (coord.), *Manual de justicia constitucional ecuatoriana (*Quito-Ecuador: Centro de Estudios y Difusión del Derecho Constitucional, 2013.

Zamudio, María de Lourdes. “El marco latinoamericano y Ley de Protección de Datos Personales en Perú”, *Revista Internacional de Protección de Datos Personales*, No. 1. 2012.

Zavala Egas, Jorge. *Derecho Constitucional, Neoconstitucionalismo y Argumentación Jurídica*. Quito-Ecuador: Edilex S.A. Editores, 2010.

Zavaleta, Morena. “El derecho al olvido digital en la Ley de Protección de Datos Personales de Nicaragua (Ley 787)”, *Revista Latinoamericana de Protección de* Datos Personales, No. 2. 2014.

Zeledón Arancibia, Noelia. “La posible implementación de la portabilidad numérica en Nicaragua”, Revista de Derecho, No. 18. 2015.ISSN 1993-4505.

**Instrumentos internacionales**

Estándares de protección de datos personales de 2017 para los Estados Iberoamericanos. Recuperado de: https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf

Guía Legislativa para los estados miembros de la OEA (Principios de Privacidad y Protección de Datos Personales en las Américas): Recuperado de: http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

Memorándum de Montevideo del 2009, sobre protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes. Recuperado de: http://www.iijusticia.org/Memo.htm

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Recuperado de: https://www.boe.es/doue/2016/119/L00001-00088.pdf

Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), Adopted on 13 April 2016, 9.

**Referencias legales**

Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de España. Recuperado de: https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales de España. Recuperado de: https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Ley Orgánica de Protección de Datos Personales de Ecuador. 2021

Proyecto de Ley Orgánica de la protección de los derechos a la intimidad y privacidad sobre los datos personales de Ecuador. 2016.

Proyecto de Ley Orgánica de Protección de Datos Personales de Ecuador. 2019

**ANEXOS**

Ley Orgánica de Protección de Datos Personales de Ecuador

Proyectos de Ley de Ecuador

QUINTO SUPLEMENTO

REGISTRO OFICIAL
ÓRGANO DE LA REPÚBLICA DEL ECUADOR

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

**ASAMBLEA NACIONAL**

# LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

Año II - Nº 459 - 70 páginas
Quito, miércoles 26 de mayo de 2021

**PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR**

Oficio No. T. 680-SGJ-21-0263

Quito, 21 de mayo de 2021

Señor Ingeniero
Hugo Del Pozo Barrezueta
**DIRECTOR DEL REGISTRO OFICIAL**
En su despacho

De mi consideración:

Con oficio número PAN-CLC-2021-0384 de 11 de mayo de 2021, el señor Ingeniero César Litardo Caicedo, Presidente de la Asamblea Nacional, remitió el proyecto de **LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES.**

Dicho proyecto de ley ha sido sancionado por el señor Presidente de la República, el día de hoy, por lo que, conforme a lo dispuesto en los artículos 137 de la Constitución de la República y 63 de la Ley Orgánica de la Función Legislativa, se la remito a usted en original y en copia certificada, junto con el certificado de discusión, para su correspondiente publicación en el Registro Oficial.

Adicionalmente, agradeceré a usted que, una vez realizada la respectiva publicación, se sirva remitir el ejemplar original a la Asamblea Nacional para los fines pertinentes.

Atentamente,

Dra. Johana Pesántez Benítez
**SECRETARIA GENERAL JURÍDICA**

**C.C.: Señora Abogada Guadalupe Llori Abarca, PRESIDENTA DE LA ASAMBLEA NACIONAL**

**Adjunto lo indicado**

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

## CERTIFICACIÓN

En mi calidad de Secretario General de la Asamblea Nacional, me permito **CERTIFICAR** que los días 09 y 11 de febrero 2021, la Asamblea Nacional discutió en primer debate el **"PROYECTO LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES** y, en segundo debate el día 10 de mayo de 2021, siendo en esta última fecha finalmente aprobado.

Quito, 11 de mayo de 2021.

**DR. JAVIER RUBIO DUQUE**
Secretario General

REPÚBLICA DEL ECUADOR
*Asamblea Nacional*

**EL PLENO**

**CONSIDERANDO**

**Que,** el artículo 1 de la Constitución de la República dispone que el *"Estado ecuatoriano es un Estado constitucional de derechos y justicia, social, democrático (...)"*;

**Que,** el artículo 3 en sus numerales 1, 5 y 8 de la Carta Magna determinan que son deberes primordiales del Estado *"1. Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales, en particular la educación, la salud, la alimentación, la seguridad social y el agua para sus habitantes. 5. Planificar el desarrollo nacional, erradicar la pobreza, promover el desarrollo sustentable y la redistribución equitativa de los recursos y la riqueza, para acceder al buen vivir. 8. Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción."*;

**Que,** el numeral 1 del artículo 11 de la Norma Suprema establece que *"Los derechos se podrán ejercer, promover y exigir de forma individual o colectiva ante las autoridades competentes; estas autoridades garantizarán su cumplimiento."*;

**Que,** el numeral 2 del artículo 11 de la Norma Suprema prescribe que *"Todas las personas son iguales y gozarán de los mismos derechos y oportunidades"*;

**Que,** el numeral 3 del artículo 11 de la Constitución de la República preceptúa que *"Los derechos y garantías establecidas en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor público, administrativo o judicial, de oficio o a petición de parte"*;

**Que,** el numeral 8 del artículo 11 de la Norma Suprema dispone que: *"El contenido de los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos, no excluirá los demás derechos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, que sean necesarios para su pleno desenvolvimiento. Será inconstitucional cualquier acción u omisión de*

*carácter regresivo que disminuya, menoscabe o anule injustificadamente el ejercicio de los derechos";*

**Que,** el artículo 16 numerales 1 y 2 de la Carta Magna determina que *"Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos; 2. El acceso universal a las tecnologías de información y comunicación";*

**Que,** el artículo 17 numeral 2 de la Norma Suprema preceptúa que *"El Estado fomentará pluralidad y la diversidad en la comunicación, y al efecto: 2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de la información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada";*

**Que,** el artículo 26 de la Constitución de la República reconoce que *"La educación es un derecho de las personas a lo largo de su vida y un deber inexcusable el Estado. Constituye un área prioritaria de la política pública y de la inversión estatal, garantía de la igualdad e inclusión social y condición indispensable para el buen vivir. Las personas, las familias y la sociedad tienen el derecho y la responsabilidad de participar en el proceso educativo";*

**Que,** el artículo 35 de la Carta Magna establece que *"Las personas adultas mayores, niñas, niños y adolescentes, mujeres embarazadas, personas con discapacidad, personas privadas de libertad y quienes adolezcan de enfermedades catastróficas o de alta complejidad, recibirán atención prioritaria y especializada en los ámbitos públicos y privado. La misma atención prioritaria recibirán las personas en situación de riesgo, las víctimas de violencia doméstica y sexual, maltrato infantil, desastres naturales o antropogénicos. El Estado prestará especial protección a las personas en condición de doble vulnerabilidad ";*

**Que,** el artículo 44 de la Norma Suprema dispone que *"El Estado, la sociedad, y la familia promoverán de forma prioritaria el desarrollo integral de los niñas, niños y adolescentes, y asegurarán el ejercicio pleno de sus derechos, se atenderá al principio de su interés superior y sus derechos prevalecerán*

*sobre los de las demás personas. Las niñas, niños y adolescentes tendrán derecho a su desarrollo integral, entendido como proceso de crecimiento, maduración y despliegue de su intelecto y de sus capacidades, potencialidades y aspiraciones, en un entorno familiar, escolar, social y comunitario de efectividad y seguridad. Este entorno permitirá la satisfacción de sus necesidades sociales, afectivo-emocionales y culturales, con el apoyo de políticas intersectoriales nacionales y locales.";*

**Que,** el artículo 66 numeral 19 de la Constitución de la República reconoce y garantiza a las personas: "*19. El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley*";

**Que,** el numeral 6 del artículo 76 de la Carta Magna determina que "*En todo proceso que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas: 6. La ley establecerá la debida proporcionalidad entre las infracciones y las sanciones penales, administrativas o de otra naturaleza.*";

**Que,** el artículo 92 de la Norma Suprema prescribe que: "*Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados*";

**Que,** el articulo 227 de la Constitución de la República establece que: *"La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.";*

**Que,** el articulo 277 de la Constitución de la República determina que: *"Para la consecución del buen vivir, serán deberes generales del Estado: 1. Garantizar los derechos de las personas, las colectividades y la naturaleza; 2. Dirigir, planificar y regular el proceso de desarrollo; 3. Generar y ejecutar las políticas públicas y controlar y sancionar su incumplimiento; 4. Producir bienes, crear y mantener infraestructura y proveer servicios públicos; 5. Impulsar el desarrollo de las actividades económicas mediante un orden jurídico e instituciones políticas que las promuevan, fomenten y defiendan mediante el cumplimiento de la Constitución y la ley; 6. Promover e impulsar la ciencia, la tecnología, las artes, los saberes ancestrales y en general las actividades de la iniciativa creativa, comunitaria, asociativa, cooperativa y privada.";*

**Que,** el articulo 417 de la Norma Suprema dispone que *"Los tratados internacionales ratificados por el Ecuador se sujetarán a lo establecido en la Constitución. En el caso de los tratados y otros instrumentos internacionales de derechos humanos se aplicarán los principios pro ser humano, de no restricción de derechos, de aplicabilidad directa y de cláusula abierta establecida en la Constitución";*

**Que,** el numeral 3 del articulo 423 de la Constitución de la República prevé que *"La integración en especial con los países de Latinoamérica y el Caribe será un objetivo estratégico del Estado. En todas las instancias y procesos de integración, el Estado ecuatoriano se comprometerá a 3 Fortalecer la armonización de las legislaciones nacionales con énfasis en los derechos (...), de acuerdo con los principios de progresividad y no regresividad.";*

**Que,** el articulo 424 de la Carta Magna prescribe que *"La Constitución es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico. Las normas y los actos del poder público deberán mantener conformidad con las disposiciones constitucionales, en caso contrario carecerán de eficacia jurídica. La Constitución y los tratados internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los*

*contenidos en la Constitución, prevalecerán sobre cualquier otra norma jurídica o acto del poder público.*";

**Que,** la Resolución 45/95 de 14 de diciembre de 1990 de la Organización de las Naciones Unidas adopta principios rectores para la reglamentación de los ficheros computarizados de datos personales, garantías mínimas que deberán preverse en legislaciones nacionales para efectivizar este derecho;

**Que,** uno de los ejes de la Estrategia acordada en el año 2016 de la red Iberoamericana de Datos Personales 2020 consiste en "*Impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetros para futuras regulaciones o para revisión de las existentes en materia de protección de datos personales*";

**Que,** el 20 de junio de 2017 se aprobaron los Estándares de Protección de Datos Personales para los Estados Iberoamericanos;

**Que,** el Comité Jurídico Interamericano de la Organización de Estados Americanos adoptó la propuesta de declaración de principios de privacidad y protección de datos personales en las Américas;

**Que,** la Organización de Estados Americanos el 27 de marzo de 2015 desarrolló el Proyecto de Ley Modelo sobre Protección de datos Personales;

**Que,** la protección de datos personales forma parte de los ejes estratégicos para la construcción de la sociedad de la información y el conocimiento en el Ecuador conforme el Libro Blanco de la Sociedad de la Información y del Conocimiento 2018;

**Que,** la Acción Estratégica clave del enfoque para Gobierno de protección de datos personales del Eje 6 del Plan Nacional de la Sociedad de la Información y del Conocimiento 2018-2021, es "*Promulgar una ley orgánica de protección de datos personales para garantizar el derecho constitucional.*";

**Que,** el principio de Legalidad de la Carta Iberoamericana de Gobierno Electrónico del año 2007 establece que "*(...) el uso de comunicaciones electrónicas promovidas por la Administración Pública deberá tener observancia de las normas en materia de protección de datos personales*",

con el objetivo de precautelar el derecho que tienen los ciudadanos a relacionarse electrónicamente con el Estado;

**Que,** la Estrategia 3 del Programa de Gobierno Abierto del Plan Nacional de Gobierno Electrónico apunta a "Impulsar la protección de la información y datos personales"; y,

En uso de la atribución que le confiere el número 6 del artículo 120 de la Constitución de la República, expide la siguiente:

## LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

### CAPÍTULO I

### ÁMBITO DE APLICACIÓN INTEGRAL

**Artículo 1.- Objeto y finalidad.-** El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.

**Artículo 2.- Ámbito de aplicación material.-** La presente ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. La ley no será aplicable a:

a) Personas naturales que utilicen estos datos en la realización de actividades familiares o domésticas;

b) Personas fallecidas, sin perjuicio de lo establecido en el artículo 28 de la presente Ley;

c) Datos anonimizados, en tanto no sea posible identificar a su titular. Tan pronto los datos dejen de estar disociados o de ser anónimos, su tratamiento estará sujeto al cumplimiento de las obligaciones de esta ley, especialmente la de contar con una base de licitud para continuar tratando los datos de manera no anonimizada o disociada;

d) Actividades periodísticas y otros contenidos editoriales;

e) Datos personales cuyo tratamiento se encuentre regulado en normativa especializada de igual o mayor jerarquía en materia de gestión de riesgos por desastres naturales; y, seguridad y defensa del Estado, en cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad;

f) Datos o bases de datos establecidos para la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, llevado a cabo por los organismos estatales competentes en cumplimiento de sus funciones legales. En cualquiera de estos casos deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad; y

g) Datos que identifican o hacen identificable a personas jurídicas.

Son accesibles al público y susceptibles de tratamiento los datos personales referentes al contacto de profesionales y los datos de comerciantes, representantes y socios y accionistas de personas jurídicas y servidores públicos, siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo y se trate de nombres y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, y, número de teléfono profesional. En el caso de los servidores públicos, además serán de acceso público y susceptibles de tratamiento de datos, el histórico y vigente de la declaración patrimonial y de su remuneración.

**Artículo 3.- Ámbito de aplicación territorial.**- Sin perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia, se aplicará la presente Ley cuando:

1. El tratamiento de datos personales se realice en cualquier parte del territorio nacional;

2. El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional;

3. Se realice tratamiento de datos personales de titulares que residan en el Ecuador por parte de un responsable o encargado no establecido en el Ecuador, cuando las actividades del tratamiento estén relacionadas con: 1) La oferta de

bienes o servicios a dichos titulares, independientemente de si a estos se les requiere su pago, o, 2) del control de su comportamiento, en la medida en que este tenga lugar en el Ecuador; y,

4. Al responsable o encargado del tratamiento de datos personales, no domiciliado en el territorio nacional, le resulte aplicable la legislación nacional en virtud de un contrato o de las regulaciones vigentes del derecho internacional público.

**Artículo 4.- Términos y definiciones.-** Para los efectos de la aplicación de la presente Ley se establecen las siguientes definiciones:

**Autoridad de Protección de Datos Personales:** Autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales.

**Anonimización:** La aplicación de medidas dirigidas a impedir la identificación o reidentificación de una persona natural, sin esfuerzos desproporcionados.

**Base de datos o fichero:** Conjunto estructurado de datos cualquiera que fuera la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica.

**Consentimiento:** Manifestación de la voluntad libre, especifica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos.

**Dato biométrico:** Dato personal único, relativo a las características físicas o fisiológicas, o conductas de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros.

**Dato genético:** Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo.

**Dato personal:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente.

**Datos personales crediticios:** Datos que integran el comportamiento económico de personas naturales, para analizar su capacidad financiera.

**Datos relativos a:** etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos, datos relativos a las personas apátridas y refugiados que requieren protección internacional, y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

**Datos relativos a la salud:** datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.

**Datos sensibles:** Datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales.

**Delegado de protección de datos:** Persona natural encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable del tratamiento de datos.

**Destinatario:** Persona natural o jurídica que ha sido comunicada con datos personales.

**Elaboración de perfiles:** Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o estándares relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación, movimiento físico de una persona, entre otros.

**Encargado del tratamiento de datos personales:** Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales.

**Entidad Certificadora:** Entidad reconocida por la Autoridad de Protección de Datos Personales, que podrá, de manera no exclusiva, proporcionar certificaciones en materia de protección de datos personales.

**Fuente accesible al público:** Bases de datos que pueden ser consultadas por cualquier persona, cuyo acceso es público, incondicional y generalizado.

**Responsable de tratamiento de datos personales:** persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales.

**Sellos de protección de datos personales:** Acreditación que otorga la entidad certificadora al responsable o al encargado del tratamiento de datos personales, de haber implementado mejores prácticas en sus procesos, con el objetivo de promover la confianza del titular, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

**Seudonimización:** Tratamiento de datos personales de manera tal que ya no puedan atribuirse a un titular sin utilizar información adicional, siempre que dicha información adicional, figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

**Titular:** Persona natural cuyos datos son objeto de tratamiento.

**Transferencia o comunicación:** Manifestación, declaración, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que comuniquen deben ser exactos, completos y actualizados.

**Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

**Vulneración de la seguridad de los datos personales:** Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales.

**Artículo 5.- Integrantes del sistema de protección de datos personales.-** Son parte del sistema de protección de datos personales, los siguientes:

1) Titular;
2) Responsable del tratamiento;
3) Encargado del tratamiento;
4) Destinatario;
5) Autoridad de Protección de Datos Personales; y,
6) Delegado de protección de datos personales.

**Artículo 6.- Normas aplicables al ejercicio de derechos.-** El ejercicio de los derechos previstos en esta Ley se canalizará a través del responsable del tratamiento, Autoridad de Protección de Datos Personales o jueces competentes, de conformidad con el procedimiento establecido en la presente Ley y su respectivo Reglamento de aplicación. El Reglamento a esta Ley u otra norma secundaria no podrán limitar al ejercicio de los derechos.

**Artículo 7.- Tratamiento legítimo de datos personas.-** El tratamiento será legítimo y lícito si se cumple con alguna de las siguientes condiciones:

1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades específicas;
2) Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal;
3) Que sea realizado por el responsable del tratamiento, por orden judicial, debiendo observarse los principios de la presente ley;
4) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad;
5) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el

responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado;

6) Para proteger intereses vitales, del interesado o de otra persona natural, como su vida, salud o integridad,
7) Para tratamiento de datos personales que consten en bases de datos de acceso público; u,
8) Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma.

**Artículo 8.- Consentimiento.-** Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea:

1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento;
2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento;
3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia,
4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular.

El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento.

El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos.

Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste que dicho consentimiento se otorga para todas ellas.

**Artículo 9.- Interés legítimo.-** Cuando el tratamiento de datos personales tiene como fundamento el interés legítimo:

a) Únicamente podrán ser tratados los datos que sean estrictamente necesarios para la realización de la finalidad.

b) El responsable debe garantizar que el tratamiento sea transparente para el titular.

c) La Autoridad de Protección de Datos puede requerir al responsable un informe con de riesgo para la protección de datos en el cual se verificará si no hay amenazas concretas a las expectativas legítimas de los titulares y a sus derechos fundamentales.

## CAPÍTULO II

## PRINCIPIOS

**Artículo 10.- Principios.-** Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de:

**a) Juridicidad.-** Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la presente Ley, su Reglamento y la demás normativa y jurisprudencia aplicable.

**b) Lealtad.-** El tratamiento de datos personales deberá ser leal, por lo que para los titulares debe quedar claro que se están recogiendo, utilizando, consultando o tratando de otra manera, datos personales que les conciernen, así como las formas en que dichos datos son o serán tratados.

En ningún caso los datos personales podrán ser tratados a través de medios o para fines, ilícitos o desleales.

**c) Transparencia.-** El tratamiento de datos personales deberá ser transparente, por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro.

Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia.

**d) Finalidad.-** Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular; no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que

concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.

El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Para ello, habrá de considerarse el contexto en el que se recogieron los datos, la información facilitada al titular en ese proceso y, en particular, las expectativas razonables del titular basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los titulares del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

**e) Pertinencia y minimización de datos personales.-** Los datos personales deben ser pertinentes y estar limitados a lo estrictamente necesario para el cumplimiento de la finalidad del tratamiento.

**f) Proporcionalidad del tratamiento.-** El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo con relación a las finalidades para las cuales hayan sido recogidos o a la naturaleza misma de las categorías especiales de datos.

**g) Confidencialidad.-** El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no debe tratarse o comunicarse para un fin distinto para el cual fueron recogidos, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.

Para tal efecto, el responsable del tratamiento deberá adecuar las medidas técnicas organizativas para cumplir con este principio.

**h) Calidad y exactitud.-** Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros, precisos, completos, comprobables, claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

En caso de tratamiento por parte de un encargado, la calidad y exactitud será obligación del responsable del tratamiento de datos personales.

Siempre que el responsable del tratamiento haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, no le será imputable la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del titular.

b) Hubiesen sido obtenidos por el responsable de un intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario que recoja en nombre propio los datos de los afectados para su transmisión al responsable.

c) Fuesen obtenidos de un registro público por el responsable.

**i) Conservación.-** Los datos personales serán conservados durante un tiempo no mayor al necesario para cumplir con la finalidad de su tratamiento.

Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica.

La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales, oportunas y necesarias, para salvaguardar los derechos previstos en esta norma.

**j) Seguridad de datos personales.-** Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.

**k) Responsabilidad proactiva y demostrada.-** El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley, para lo cual, además de

lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y coregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.

El responsable del tratamiento de datos personales está obligado a rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales.

El responsable del tratamiento de datos personales deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la presente Ley.

**l) Aplicación favorable al titular.-** En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.

**m) Independencia del control.-** Para el efectivo ejercicio del derecho a la protección de datos personales, y en cumplimiento de las obligaciones de protección de los derechos que tiene el Estado, la Autoridad de Protección de Datos deberá ejercer un control independiente, imparcial y autónomo, así como llevar a cabo las respectivas acciones de prevención, investigación y sanción.

## CAPÍTULO III

## DERECHOS

**Artículo 11.- Normativa especializada.-** Los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, sectores regulados por normativa específica, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente, estarán sujetos a los principios establecidos en sus propias normas y los principios establecidos en esta Ley, en los casos que corresponda y sea de aplicación favorable. En todo caso deberá darse cumplimiento a los estándares internacionales en la materia de derechos humanos y a los principios

de esta ley, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad.

**Artículo 12.- Derecho a la información.**- El titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparente por cualquier medio sobre:

1) Los fines del tratamiento;
2) La base legal para el tratamiento;
3) Tipos de tratamiento;
4) Tiempo de conservación;
5) La existencia de una base de datos en la que constan sus datos personales;
6) El origen de los datos personales cuando no se hayan obtenido directamente del titular;
7) Otras finalidades y tratamientos ulteriores;
8) Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluirá: dirección del domicilio legal, numero de teléfono y correo electrónico;
9) Cuando sea del caso, identidad y datos de contacto del delegado de protección de datos personales, que incluirá: dirección domiciliaria, número de teléfono y correo electrónico;
10) Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de estas y las garantías de protección establecidas;
11) Las consecuencias para el titular de los datos personales de su entrega o negativa a ello;
12) El efecto de suministrar datos personales erróneos o inexactos;
13) La posibilidad de revocar el consentimiento;
14) La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas.
15) Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite;

16) Dónde y cómo realizar sus reclamos ante el responsable del tratamiento de datos personales y la Autoridad de Protección de Datos Personales, y;

17) La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

En el caso que los datos se obtengan directamente del titular, la información deberá ser comunicada de forma previa a este, es decir, en el momento mismo de la recogida del dato personal.

Cuando los datos personales no se obtuvieren de forma directa del titular o fueren obtenidos de una fuente accesible al público, el titular deberá ser informado dentro de los siguientes treinta (30) días o al momento de la primera comunicación con el titular, cualquiera de las dos circunstancias que ocurra primero. Se le deberá proporcionar información expresa, inequívoca, transparente, inteligible, concisa, precisa y sin barreras técnicas.

La información proporcionada al titular podrá transmitirse de cualquier modo comprobable en un lenguaje claro, sencillo y de fácil comprensión, de preferencia propendiendo a que pueda ser accesible en la lengua de su elección.

En el caso de productos o servicios dirigidos, utilizados o que pudieran ser utilizados por niñas, niños y adolescentes, la información a la que hace referencia el presente artículo será proporcionada a su representante legal conforme a lo dispuesto en la presente Ley.

**Artículo 13.- Derecho de acceso.-** El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna. El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el ejercicio de este derecho, el cual deberá ser atendido dentro del plazo de quince (15) días.

El derecho de acceso no podrá ejercerse de forma tal que constituya abuso del derecho.

**Artículo 14.- Derecho de rectificación y actualización.-** El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos.

Para tal efecto, el titular deberá presentar los justificativos del caso, cuando sea pertinente. El responsable de tratamiento deberá atender el requerimiento en un plazo de quince (15) días y en este mismo plazo, deberá informar al destinatario de los datos, de ser el caso, sobre la rectificación, a fin de que lo actualice.

**Artículo 15.- Derecho de eliminación.-** El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales, cuando:

1) El tratamiento no cumpla con los principios establecidos en la presente ley;
2) El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;
3) Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;
4) Haya vencido el plazo de conservación de los datos personales;
5) El tratamiento afecte derechos fundamentales o libertades individuales;
6) Revoque el consentimiento prestado o señale no haberlo otorgado para uno o varios fines específicos, sin necesidad de que medie justificación alguna; o,
7) Exista obligación legal.

El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, hacer ilegible, o dejar irreconocibles de forma definitiva y segura los datos personales. Esta obligación la deberá cumplir en el plazo de quince (15) días de recibida la solicitud por parte del titular y será gratuito.

**Artículo 16.- Derecho de oposición.-** El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en los siguientes casos:

1) No se afecten derechos y libertades fundamentales de terceros, la ley se lo permita y no se trate de información pública, de interés público o cuyo tratamiento está ordenado por la ley.
2) El tratamiento de datos personales tenga por objeto la mercadotecnia directa; el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles; en cuyo caso los datos personales dejarán de ser tratados para dichos fines.

3) Cuando no sea necesario su consentimiento para el tratamiento como consecuencia de la concurrencia de un interés legítimo, previsto en el artículo 7, y se justifique en una situación concreta personal del titular, siempre que una ley no disponga lo contrario.

El responsable de tratamiento dejará de tratar los datos personales en estos casos, salvo que acredite motivos legítimos e imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del titular, o para la formulación, el ejercicio o la defensa de reclamaciones.

Esta solicitud deberá ser atendida dentro del plazo de quince (15) días

**Artículo 17.- Derecho a la portabilidad.-** El titular tiene el derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, inter-operable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables. La Autoridad de Protección de Datos Personales deberá dictar la normativa para el ejercicio del derecho a la portabilidad.

El titular podrá solicitar que el responsable del tratamiento realice la transferencia o comunicación de sus datos personales a otro responsable del tratamiento en cuanto fuera técnicamente posible y sin que el responsable pueda aducir impedimento de cualquier orden con el fin de ralentizar el acceso, la transmisión o reutilización de datos por parte del titular o de otro responsable del tratamiento. Luego de completada la transferencia de datos, el responsable que lo haga procederá a su eliminación, salvo que el titular disponga su conservación. El responsable que ha recibido la información asumirá las responsabilidades contempladas en esta Ley.

Para que proceda el derecho a la portabilidad de datos es necesario que se produzca al menos una de las siguientes condiciones:

1) Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos. La transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible; en caso contrario los datos deberán ser transmitidos directamente al titular.

2) Que el tratamiento se efectúe por medios automatizados;

3) Que se trate de un volumen relevante de datos personales, según los parámetros definidos en el reglamento de la presente ley; o,

4) Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social.

Esta transferencia o comunicación debe ser económica y financieramente eficiente, expedita y sin trabas.

No procederá este derecho cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

**Artículo 18.- Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad.-** Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad. No proceden los derechos de rectificación, actualización, eliminación, oposición, anulación y portabilidad, en los siguientes casos:

1) Si el solicitante no es el titular de los datos personales o su representante legal no se encuentre debidamente acreditado;

2) Cuando los datos son necesarios para el cumplimiento de una obligación legal o contractual;

3) Cuando los datos son necesarios para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente;

4) Cuando los datos son necesarios para la formulación, ejercicio o defensa de reclamos o recursos;

5) Cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros y ello sea acreditado por el responsable de la base de datos al momento de dar respuesta al titular a su solicitud de ejercicio del derecho respectivo;

6) Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso, debidamente notificadas;

7) Cuando los datos son necesarios para ejercer el derecho a la libertad de expresión y opinión;

8) Cuando los datos son necesarios para proteger el interés vital del interesado o de otra persona natural;

9) En los casos en los que medie el interes público, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta ley y a los criterios de legalidad, proporcionalidad y necesidad;

10) En el tratamiento de datos personales que sean necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.

**Artículo 19.- Derecho a la suspensión del tratamiento.-** El titular tendrá derecho a obtener del responsable del tratamiento la suspensión del tratamiento de los datos, cuando se cumpla alguna de las condiciones siguientes:

1) Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos;
2) El tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;
3) El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; y,
4) Cuando el interesado se haya opuesto al tratamiento en virtud del artículo 31 de la presente ley, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

De existir negativa por parte del responsable o encargado del tratamiento de datos personales, y el titular recurra por dicha decisión ante la Autoridad de Protección de Datos Personales, esta suspensión se extenderá hasta la resolución del procedimiento administrativo.

Cuando el titular impugne la exactitud de los datos personales, mientras el responsable de tratamiento verifica la exactitud de los mismos, deberá colocarse en la base de datos, en donde conste la información impugnada, que ésta ha sido objeto de inconformidad por parte del titular.

El responsable de tratamiento podrá tratar los datos personales, que han sido objeto del ejercicio del presente derecho por parte del titular, únicamente, en los siguientes supuestos: para la formulación, el ejercicio o la defensa de reclamaciones; con el objeto de proteger los derechos de otra persona natural o jurídica o por razones de interés público importante.

**Artículo 20.- Derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.-** El titular tiene derecho a no ser sometido a una decisión basada única o parcialmente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales, para lo cual podrá:

a. Solicitar al responsable del tratamiento una explicación motivada sobre la decisión tomada por el responsable o encargado del tratamiento de datos personales;
b. Presentar observaciones;
c. Solicitar los criterios de valoración sobre el programa automatizado; o,
d. Solicitar al responsable información sobre los tipos de datos utilizados y la fuente de la cual han sido obtenidos los mismos;
e. Impugnar la decisión ante el responsable o encargado del tratamiento

No se aplicará este derecho cuando:

1. La decisión es necesaria para la celebración o ejecución de un contrato entre el titular y el responsable o encargado del tratamiento de datos personales;
2. Está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad técnica competente, para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular; o,
3. Se base en el consentimiento explícito del titular.
4. La decisión no conlleve impactos graves o riesgos verificables para el titular.

No se podrá exigir la renuncia a este derecho en forma adelantada a través de contratos de adhesión masivos. A más tardar en el momento de la primera

comunicación con el titular de los datos personales, para informar una decisión basada únicamente en valoraciones automatizadas, este derecho le será informado explícitamente por cualquier medio idóneo.

**Artículo 21.- Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas.-** Además de los presupuestos establecidos en el derecho a no ser objeto de una decisión basada única o parcialmente en valoraciones automatizadas, no se podrán tratar datos sensibles o datos de niñas, niños y adolescentes a menos que se cuente con la autorización expresa del titular o de su representante legal; o, cuando dicho tratamiento esté destinado a salvaguardar un interés público esencial, el cual se evalúe en atención a los estándares internacionales de derechos humanos, y como mínimo satisfaga los criterios de legalidad, proporcionalidad y necesidad, y además incluya salvaguardas específicas para proteger los derechos fundamentales de los interesados.

Los adolescentes, en ejercicio progresivo de sus derechos, a partir de los 15 años, podrán otorgar, en calidad de titulares, su consentimiento explícito para el tratamiento de sus datos personales, siempre que se les especifique con claridad sus fines.

**Artículo 22.- Derecho de consulta.-** Las personas tienen derecho a la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales, de conformidad con la presente Ley.

**Artículo 23.- Derecho a la educación digital.-** Las personas tienen derecho al acceso y disponibilidad del conocimiento, aprendizaje, preparación, estudio, formación, capacitación, enseñanza e instrucción relacionados con el uso y manejo adecuado, sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación, en estricto apego a la dignidad e integridad humana, los derechos fundamentales y libertades individuales con especial énfasis en la intimidad, la vida privada, autodeterminación informativa, identidad y reputación en línea, ciudadanía digital y el derecho a la protección de datos personales, así como promover una cultura sensibilizada en el derecho de protección de datos personales.

El derecho a la educación digital tendrá un carácter inclusivo sobre todo en lo que respecta a las personas con necesidades educativas especiales.

El sistema educativo nacional, incluyendo el sistema de educación superior, garantizará la educación digital no solo a favor de los estudiantes de todos los niveles sino también de los docentes, debiendo incluir dicha temática en su proceso de formación.

**Artículo 24.- Ejercicio de derechos.-** El Estado, entidades educativas, organizaciones de la sociedad civil, proveedores de servicios de la sociedad de la información y el conocimiento, y otros entes relacionados, dentro del ámbito de sus relaciones, están obligados a proveer información y capacitación relacionadas con el uso y tratamiento responsable, adecuado y seguro de datos personales de niñas, niños y adolescentes, tanto a sus titulares como a sus representantes legales, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

Los adolescentes mayores de doce (12) años y menores de quince (15) años, así como las niñas y niños, para el ejercicio de sus derechos necesitarán de su representante legal. Los adolescentes mayores de quince (15) años y menores de dieciocho (18) años, podrán ejercitarlos de forma directa ante la Autoridad de Protección de Datos Personales o ante el responsable de la base de datos personales del tratamiento.

Los derechos del titular son irrenunciables. Será nula toda estipulación en contrario.

## CAPÍTULO IV

## CATEGORÍAS ESPECIALES DE DATOS

**Artículo 25.- Categorías especiales de datos personales.-** Se considerarán categorías especiales de datos personales, los siguientes:

a) Datos sensibles;
b) Datos de niñas, niños y adolescentes;
c) Datos de salud; y,
d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.

**Artículo 26.- Tratamiento de datos sensibles.-** Queda prohibido el tratamiento de datos personales sensibles salvo que concurra alguna de las siguientes circunstancias:

a) El titular haya dado su consentimiento explícito para el tratamiento de sus datos personales, especificándose claramente sus fines.
b) El tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del titular en el ámbito del Derecho laboral y de la seguridad y protección social.
c) El tratamiento es necesario para proteger intereses vitales del titular o de otra persona natural, en el supuesto de que el titular no esté capacitado, física o jurídicamente, para dar su consentimiento.
d) El tratamiento se refiere a datos personales que el titular ha hecho manifiestamente públicos.
e) El tratamiento se lo realiza por orden de autoridad judicial.
f) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular.
g) Cuando el tratamiento de los datos de salud se sujete a las disposiciones contenidas en la presente ley.

**Artículo 27.- Datos personales de personas fallecidas.-** Los titulares de derechos sucesorios de las personas fallecidas, podrán dirigirse al responsable del tratamiento de datos personales con el objeto de solicitar el acceso, rectificación y actualización o eliminación de los datos personales del causante, siempre que el titular de los datos no haya, en vida, indicado otra utilización o destino para sus datos.

Las personas o instituciones que la o el fallecido haya designado expresamente para ello, podrán también solicitar con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste; y, en su caso, su rectificación, actualización o eliminación.

En caso de fallecimiento de niñas, niños, adolescentes o personas que la ley reconozca como incapaces, las facultades de acceso, rectificación, actualización o eliminación, podrán ser ejercidas por quien hubiese sido su último representante legal. El Reglamento a la presente ley establecerá los mecanismos para el ejercicio de las facultades enunciadas en el presente artículo.

Artículo 28.- Datos crediticios.- Salvo prueba en contrario será legítimo y lícito el tratamiento de datos destinados a informar sobre la solvencia patrimonial o crediticia, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor. Tales datos pueden ser utilizados solamente para esa finalidad de análisis y no serán comunicados o difundidos, ni podrán tener cualquier finalidad secundaria.

La protección de datos personales crediticios se sujetará a lo previsto en la presente ley, en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales.

Sin perjuicio de lo anterior, en ningún caso podrán comunicarse los datos crediticios relativos a obligaciones de carácter económico, financiero, bancario o comercial una vez transcurridos cinco años desde que la obligación a la que se refieran se haya hecho exigible.

**Artículo 29- Derechos de los Titulares de Datos Crediticios.-**

1. Sin perjuicio de los derechos reconocidos en esta Ley, los Titulares de Datos Crediticios tienen los siguientes derechos:

a) Acceder de forma personal a la información de la cual son titulares;
b) Que el reporte de crédito permita conocer de manera clara y precisa la condición en que se encuentra su historial crediticio; y,
c) Que las fuentes de información actualicen, rectifiquen o eliminen, según el caso, la información que fuese ilícita, falsa, inexacta, errónea, incompleta o caduca

2. Sobre el derecho de acceso por el Titular del Dato Crediticio, éste será gratuito, cuantas veces lo requiera, respecto de la información que sobre sí mismos esté registrada ante los prestadores de servicios de referencia crediticia y a través de los siguientes mecanismos:

a) Observación directa a través de pantallas que los prestadores del servicio de referencia crediticia pondrán a disposición de dichos titulares; y,

b) Entrega de impresiones de los reportes que a fin de que el Titular del Dato Crediticio compruebe la veracidad y exactitud de su contenido, sin que pueda ser utilizado con fines crediticios o comerciales.

3. Sobre los derechos de actualización, rectificación o eliminación, el Titular del Dato Crediticio podrá exigir estos derechos frente a las fuentes de información mediante solicitud escrita. Las fuentes de información, dentro del plazo de quince días de presentada la solicitud, deberán resolverla admitiéndola o rechazándola motivadamente. El Titular del Dato Crediticio tiene derecho a solicitar a los prestadores del servicio de referencias crediticias que, en tanto se sigue el proceso de revisión, señalen en los reportes de crédito que emitan, que la información materia de la solicitud está siendo revisada a pedido del titular.

**Artículo 30.- Datos relativos a la salud.-** Las instituciones que conforman el Sistema Nacional de Salud y los profesionales de la salud pueden recolectar y tratar los datos relativos a la salud de sus pacientes que estén o hubiesen estado bajo tratamiento de aquellos, de acuerdo a lo previsto en la presente ley, en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales en coordinación con la autoridad sanitaria nacional.

Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este, estarán sujetas al deber de confidencialidad, de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas organizativas apropiadas. Esta obligación será complementaria del secreto profesional de conformidad con cada caso.

Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

No se requerirá el consentimiento del titular para el tratamiento de datos de salud cuando ello sea necesario por razones de interés público esencial en el ámbito de la salud, el que en todo caso deberá ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del titular;

Asimismo, tampoco se requerirá el consentimiento del titular cuando el tratamiento sea necesario por razones de interés público en el ámbito de la salud pública, como en el caso de amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, siempre y cuando se establezcan medidas adecuadas y específicas para proteger los derechos y libertades del titular y, en particular, el secreto profesional.

**Artículo 31.- Tratamiento de datos relativos a la salud.-** Todo tratamiento de datos relativos a la salud deberá cumplir con los siguientes parámetros mínimos y aquellos que determine la Autoridad de Protección de Datos Personales en la normativa emitida para el efecto:

1. Los datos relativos a la salud generados en establecimientos de salud públicos o privados, serán tratados cumpliendo los principios de confidencialidad y secreto profesional. El titular de la información deberá brindar su consentimiento previo conforme lo determina esta Ley, salvo en los casos en que el tratamiento sea necesario para proteger intereses vitales del interesado, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; o sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base de la legislación especializada sobre la materia o en virtud de un contrato con un profesional sanitario. En este último caso el tratamiento sólo podrá ser realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con la legislación especializada sobre la materia o con las demás normas que al respecto pueda establecer la Autoridad.

2. Los datos relativos a la salud que se traten, siempre que sea posible, deberán ser previamente anonimizados o seudonimizados, evitando la posibilidad de identificar a los titulares de los mismos.

3. Todo tratamiento de datos de salud anonimizados deberá ser autorizado previamente por la Autoridad de Protección de Datos Personales. Para obtener la autorización mencionada, el interesado deberá presentar un protocolo técnico que contenga los parámetros necesarios que garanticen la protección de dichos datos y el informe previo favorable emitido por la Autoridad Sanitaria.

**Artículo 32.- Tratamiento de datos de salud por entes privados y públicos con fines de investigación.-** Los datos relativos a salud que consten en las instituciones que conforman el Sistema Nacional de Salud, podrán ser tratados por personas naturales y jurídicas privadas y públicas con fines de investigación científica, siempre que según el caso encuentren anonimizados, o dicho tratamiento sea autorizado por la Autoridad de Protección de Datos Personales, previo informe de la Autoridad Sanitaria Nacional.

## CAPÍTULO V

## TRANSFERENCIA O COMUNICACIÓN Y ACCESO A DATOS PERSONALES POR TERCEROS

**Artículo 33.- Transferencia o comunicación de datos personales.-** Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada dentro de una de las causales de legitimidad establecidas en esta Ley, y se cuente, además, con el consentimiento del titular.

Se entenderá que el consentimiento es informado cuando para la transferencia o comunicación de datos personales el Responsable del tratamiento haya entregado información suficiente al titular que le permita conocer la finalidad a que se destinarán sus datos y el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos.

**Artículo 34.- Acceso a datos personales por parte del encargado.-** No se considerará transferencia o comunicación en el caso de que el encargado acceda a datos personales para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido legítimamente a datos personales en estas consideraciones, será considerado encargado del tratamiento.

El tratamiento de datos personales realizado por el encargado deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas.

Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la Autoridad de Protección de Datos Personales.

El encargado será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.

**Artículo 35.- Acceso a datos personales por parte de terceros.-** No se considerará transferencia o comunicacion cuando el acceso a datos personales por un tercero sea necesario para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido a datos personales en estas condiciones debió hacerlo legitimamente.

El tratamiento de datos personales realizado por terceros deberá estar regulado por un contrato, en el que se establezca de manera clara y precisa que el encargado del tratamiento de datos personales tratará únicamente los mismos conforme las instrucciones del responsable y que no los utilizará para finalidades diferentes a las señaladas en el contrato, ni que los transferirá o comunicará ni siquiera para su conservación a otras personas.

Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales bajo la supervisión de la autoridad de protección de datos personales.

El tercero será responsable de las infracciones derivadas del incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.

**Artículo 36.- Excepciones de consentimiento para la transferencia o comunicación de datos personales.-** No es necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales, en los siguientes supuestos:

1) Cuando los datos han sido recogidos de fuentes accesibles al público;

2) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable de tratamiento y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho

tratamiento con base de datos. En este caso la transferencia o comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique;

3) Cuando los datos personales deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la norma vigente;

4) Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados o a lo menos anonimizados, y,

5) Cuando la comunicación de datos de caracter personal relativos a la salud sea necesaria para solucionar una urgencia que implique intereses vitales de su titular y este se encontrare impedido de otorgar su consentimiento.

6) Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para realizar los estudios epidemiológicos de interés público, dando cumplimiento a los estándares internacionales en la materia de derechos humanos, y como mínimo a los criterios de legalidad, proporcionalidad y necesidad. El tratamiento deberá ser de preferencia anonimizado, y en todo caso agregado, una vez pasada la urgencia de interés público.

Cuando sea requerido el consentimiento del titular para que sus datos personales sean comunicados a un tercero, este puede revocarlo en cualquier momento, sin necesidad de que medie justificación alguna.

La presente ley obligatoriamente debe ser aplicada por el destinatario, por el solo hecho de la comunicación de los datos; a menos que estos hayan sido anonimizados o sometidos a un proceso de

## CAPÍTULO VI

## SEGURIDAD DE DATOS PERSONALES

**Artículo 37.- Seguridad de datos personales.-** El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la

naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos.

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.

El responsable o encargado del tratamiento de datos personales deberá evidenciar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados

Entre otras medidas, se podrán incluir las siguientes:

1) Medidas de anonimización, seudonomización o cifrado de datos personales;
2) Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y
3) Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, y jurídica.
4) Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares internacionales para una adecuada gestión de riesgos enfocada a la protección de derechos y libertades, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

**Artículo 38.- Medidas de seguridad en el ámbito del sector público.-** El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.

El mecanismo gubernamental de seguridad de la información abarcará y aplicará a todas las instituciones del sector público, contenidas en el artículo 225 de la

Constitución de la República de Ecuador, así como a terceros que presten servicios públicos mediante concesión u otras figuras legalmente reconocidas. Estas, podrán incorporar medidas adicionales al mecanismo gubernamental de seguridad de la información.

**Artículo 39.- Protección de datos personales desde el diseño y por defecto.-** Se entiende a la protección de datos desde el diseño como el deber del responsable del tratamiento de tener en cuenta, en las primeras fases de concepción y diseño del proyecto, que determinados tipos de tratamientos de datos personales entrañan una serie de riesgos para los derechos de los titulares en atención al estado de la técnica, naturaleza y fines del tratamiento, para lo cual, implementará las medidas técnicas, organizativas y de cualquier otra índole, con miras a garantizar el cumplimiento de las obligaciones en materia de protección de datos, en los términos del reglamento.

La protección de datos por defecto hace referencia a que el responsable debe aplicar las medidas técnicas y organizativas adecuadas con miras a que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines del tratamiento, en los términos del reglamento.

**Artículo 40.- Análisis de riesgo, amenazas y vulnerabilidades.-** Para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras:

1) Las particularidades del tratamiento;
2) Las particularidades de las partes involucradas; y,
3) Las categorías y el volumen de datos personales objeto de tratamiento.

**Artículo 41.- Determinación de medidas de seguridad aplicables.-** Para determinar las medidas de seguridad, aceptadas por el estado de la técnica, a las que están obligadas el responsable y el encargado del tratamiento de los datos personales, se deberán tomar en consideración, entre otros:

1) Los resultados del análisis de riesgos, amenazas y vulnerabilidades;
2) La naturaleza de los datos personales;
3) Las características de las partes involucradas; y,
4) Los antecedentes de destrucción de datos personales, la pérdida, alteración, divulgación o impedimento de acceso a los mismos por parte del titular, sean accidentales e intencionales, por acción u omisión, así como los

antecedentes de transferencia, comunicación o de acceso no autorizado o exceso de autorización de tales datos.

El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales.

**Artículo 42.- Evaluación de impacto del tratamiento de datos personales.-** El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se haya identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleve un alto riesgo para los derechos y libertades del titular o cuando la Autoridad de Protección de Datos Personales lo requiera.

La evaluación de impacto relativa a la protección de los datos será de carácter obligatoria en caso de:

a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas naturales;

b) Tratamiento a gran escala de las categorías especiales de datos, o de los datos personales relativos a condenas e infracciones penales, o

c) Observación sistemática a gran escala de una zona de acceso público.

La Autoridad de Protección de Datos Personales establecerá otros tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos.

La evaluación de impacto deberá efectuarse previo al inicio del tratamiento de datos personales.

**Artículo 43.- Notificación de vulneración de seguridad.-** El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el

término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación.

El encargado del tratamiento deberá notificar al responsable cualquier vulneración de la seguridad de datos personales tan pronto sea posible, y a más tardar dentro del término de dos (2) días contados a partir de la fecha en la que tenga conocimiento de ella.

**Artículo 44.- Acceso a datos personales para atención a emergencias e incidentes informáticos.-** Las autoridades públicas competentes, los equipos de respuesta de emergencias informáticas, los equipos de respuesta a incidentes de seguridad informática, los centros de operaciones de seguridad, los prestadores y proveedores de servicios de telecomunicaciones y los proveedores de tecnología y servicios de seguridad, nacionales e internacionales, podrán acceder y efectuar tratamientos sobre los datos personales contenidos en las notificaciones de vulneración a las seguridades, durante el tiempo necesario, exclusivamente para la detección, análisis, protección y respuesta ante cualquier tipo de incidentes así como para adoptar e implementar medidas de seguridad adecuadas y proporcionadas a los riesgos identificados.

**Artículo 45.- Garantía del secreto de las comunicaciones y seguridad de datos personales.-** Para la correcta prestación de los servicios de telecomunicaciones y la apropiada operación de redes de telecomunicaciones, los prestadores de servicios de telecomunicaciones deben garantizar el secreto de las comunicaciones y seguridad de datos personales. Únicamente por orden judicial, los prestadores de servicios de telecomunicaciones podrán utilizar equipos, infraestructuras e instalaciones que permitan grabar los contenidos de las comunicaciones específicas dispuestas por los jueces competentes. Si se evidencia un tratamiento de grabación o interceptación de las comunicaciones no autorizadas por orden judicial, se aplicará lo dispuesto en la presente Ley.

**Artículo 46.- Notificación de vulneración de seguridad al titular.-** El responsable del tratamiento deberá notificar sin dilación la vulneración de seguridad de datos personales al titular cuando conlleve un riesgo a sus derechos fundamentales y libertades individuales, dentro del término de tres días contados a partir de la fecha en la que tuvo conocimiento del riesgo.

No se deberá notificar la vulneración de seguridad de datos personales al titular en los siguientes casos:

1. Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas organizativas o de cualquier otra índole apropiadas aplicadas a los datos personales afectados por la vulneración de seguridad que se pueda demostrar que son efectivas;

2. Cuando el responsable del tratamiento haya tomado medidas que garanticen que el riesgo para los derechos fundamentales y las libertades individuales del titular, no ocurrirá; y,

3. Cuando se requiera un esfuerzo desproporcionado para hacerlo: en cuyo caso, el responsable del tratamiento deberá realizar una comunicación pública a través de cualquier medio en la que se informe de la vulneración de seguridad de datos personales a los titulares.

La procedencia de las excepciones de los numerales 1 y 2 deberá ser calificada por la Autoridad de Protección de Datos, una vez informada esta tan pronto sea posible, y en cualquier caso dentro de los plazos contemplados en el Artículo 43.

La notificación al titular del dato objeto de la vulneración de seguridad contendrá lo señalado en el artículo 43 de esta ley.

En caso de que el responsable del tratamiento de los datos personales no cumpliese oportunamente y de modo justificado con la notificación será sancionado conforme al régimen sancionatorio previsto en esta ley.

La notificación oportuna de la violación por parte del responsable de tratamiento al titular y la ejecución oportuna de medidas de respuesta, serán consideradas atenuante de la infra

## CAPÍTULO VII

## DEL RESPONSABLE, ENCARGO Y DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

**Artículo 47.- Obligaciones del responsable y encargado del tratamiento de datos personales.-** El responsable del tratamiento de datos personales está obligado a:

1) Tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;

2) Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales o normativa sobre la materia;

3) Aplicar e implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas;

4) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;

5) Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;

6) Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;

7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas;

8) Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto;

9) Implementar la protección de datos personales desde el diseño y por defecto;

10) Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;

11) Asegurar que el encargado del tratamiento de datos personales ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional;

12) Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales;

13) Designar al Delegado de Protección de Datos Personales, en los casos que corresponda;

14) Permitir y contribuir a la realización de auditorias o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales; y,

15) Los demás establecidos en la presente Ley en su reglamento, en directrices, lineamientos, regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

El encargado de tratamiento de datos personales tendrá las mismas obligaciones que el responsable de tratamiento de datos personales, en lo que sea aplicable, de acuerdo a la presente ley y su reglamento.

**Artículo 48.- Delegado de protección de datos personales.-** Se designará un delegado de protección de datos personales en los siguientes casos:

1) Cuando el tratamiento se lleve a cabo por quienes conforman el sector público de acuerdo con lo establecido en el artículo 225 de la Constitución de la República;

2) Cuando las actividades del responsable o encargado del tratamiento de datos personales requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades del tratamiento, conforme se establezca en esta ley, el reglamento a ésta, o en la normativa que dicte al respecto la Autoridad de Protección de Datos Personales;

3) Cuando se refiera al tratamiento a gran escala de categorías especiales de datos, de conformidad con lo establecido en el reglamento de esta ley; y,

4) Cuando el tratamiento no se refiera a datos relacionados con la seguridad nacional y defensa del Estado que adolezcan de reserva ni fuesen secretos, de conformidad con lo establecido en la normativa especializada en la materia.

La Autoridad de Protección de Datos Personales podrá definir nuevas condiciones en las que deba designarse un delegado de protección de datos personales y emitirá, a dicho efecto, las directrices suficientes para su designación.

**Artículo 49.- Funciones del delegado de protección de datos personales.-** El delegado de protección de datos personales tendrá, entre otras, las siguientes funciones y atribuciones:

1) Asesorar al responsable, al personal del responsable y al encargado del tratamiento de datos personales, sobre las disposiciones contenidas en esta ley, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales;

2) Supervisar el cumplimiento de las disposiciones contenidas en esta ley, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales;

3) Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación;

4) Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos personales; y,

5) Las demás que llegase a establecer la Autoridad de Protección de Datos Personales con ocasión de las categorías especiales de datos personales.

En caso de incumplimiento de sus funciones, el delegado de protección de datos personales responderá administrativa, civil y penalmente, de conformidad con la ley.

**Artículo 50.- Consideraciones especiales para el delegado de protección de datos personales.-** Para la ejecución de las funciones del delegado de protección de datos, el responsable y el encargado de tratamiento de datos personales, deberán observar lo siguiente:

1) Garantizar que la participación del delegado de protección de datos personales, en todas las cuestiones relativas a la protección de datos personales, sea apropiada y oportuna;

2) Facilitar el acceso a los datos personales de las operaciones de tratamiento, así como todos los recursos y elementos necesarios para garantizar el correcto y libre desempeño de sus funciones;

3) Capacitar y actualizar en la materia al delegado de protección de datos personales, de conformidad con la normativa técnica que emita la Autoridad de Protección de Datos Personales;

4) No podrán destituir o sancionar al delegado de protección de datos personales por el correcto desempeño de sus funciones;

5) El delegado de protección de datos personales mantendrá relación directa con el más alto nivel ejecutivo y de decisión del responsable y con el encargado;

6) El titular de los datos personales podrá contactar al delegado de protección de datos personales con relación al tratamiento de sus datos personales a fin de ejercer sus derechos; y,

7) El delegado de protección de datos personales estará obligado a mantener la más estricta confidencialidad respecto a la ejecución de sus funciones.

Siempre que no exista conflicto con las responsabilidades establecidas en la presente ley, su reglamento, directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales, el delegado de protección de datos personales podrá desempeñar otras funciones dispuestas por el responsable o el encargado del tratamiento de datos personales.

**Artículo 51.- Registro Nacional de protección de datos personales.-** El responsable del tratamiento de datos personales deberá reportar y mantener actualizada la información ante la Autoridad de Protección de Datos Personales, sobre lo siguiente:

1) Identificación de la base de datos o del tratamiento;

2) El nombre domicilio legal y datos de contacto del responsable y encargado del tratamiento de datos personales;

3) Caracteristicas y finalidad del tratamiento de datos personales;

4) Naturaleza de los datos personales tratados;

5) Identificación, nombre, domicilio legal y datos de contacto de los destinatarios de los datos personales, incluyendo encargados y terceros;

6) Modo de interrelacionar la información registrada;

7) Medios utilizados para implementar los principios, derechos y obligaciones contenidas en la presente ley y normativa especializada;

8) Requisitos y herramientas administrativas técnicas y fisicas, organizativas y juridicas implementadas para garantizar la seguridad y protección de datos personales;

9) Tiempo de conservación de los datos.

## CAPÍTULO VIII

## DE LA RESPONSABILIDAD PROACTIVA

**Artículo 52.- Autorregulación.-** Los responsables y encargados de tratamiento de datos personales podrán, de manera voluntaria, acogerse o adherirse a códigos de conducta, certificaciones, sellos y marcas de protección, cláusulas tipo, sin que esto constituya eximente de la responsabilidad de cumplir con las disposiciones de la presente ley, su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia.

**Artículo 53.- Codigos de conducta.-** La Autoridad de Regulación y Control promoverá la elaboración de códigos de conducta por sectores, industrias, empresas, organizaciones, que tengan como fin el cumplimiento de la normativa vigente en materia de protección de datos.

Los códigos de conducta deberán tomar en cuenta las necesidades especificas de los sectores en los que se efectúe tratamiento de datos personales, así como cumplir con los requisitos que se determinen en la normativa secundaria y con las disposiciones previstas en la presente Ley, para su aprobación por la Autoridad de Regulación y Control

Los responsables o encargados de tratamiento de datos personales interesados podrán adherirse e implementar los códigos de conducta aprobados, para lo cual seguirán el procedimiento establecido en el Reglamento a la presente Ley.

**Artículo 54.- Entidades de Certificación.-** En materia de protección de datos personales las Entidades de Certificación, de manera no exclusiva y en concordancia con el artículo 52, podrán.

1) Emitir certificaciones de cumplimiento de la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia;

2) Emitir sellos de protección de datos personales;

3) Llevar a cabo auditorías de protección de datos personales, y,

4) Certificar los procesos de transferencias internacionales de datos personales.

Los resultados de las auditorías podrán ser considerados como elementos probatorios dentro de los procesos sancionatorios.

## CAPÍTULO IX

## TRANSFERENCIA O COMUNICACIÓN INTERNACIONAL DE DATOS PERSONALES

**Artículo 55.- Transferencia o comunicación internacional de datos personales.-** La transferencia o comunicación internacional de datos personales será posible si se sujeta a lo previsto en el presente capítulo, la presente Ley o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales.

**Artículo 56.- Transferencia o comunicación internacional de datos personales a países declarados como nivel adecuado de protección.-** Por principio general se podrán transferir o comunicar datos personales a países, organizaciones y personas jurídicas en general que brinden niveles adecuados de protección, y que se ajusten a la obligación de cumplimiento y garantía de estándares reconocidos internacionalmente conforme a los criterios establecidos en el Reglamento a la ley.

Cuando resulte necesario por la naturaleza de la transferencia, la Autoridad de Protección de Datos Personales podrá implementar métodos de control ex post que serán definidos en el Reglamento a la Ley. También establecerá acciones conjuntas entre las autoridades de ambos países con el objeto de prevenir, corregir o mitigar el tratamiento indebido de datos en ambos países.

Para declarar de nivel adecuado de protección a países u organizaciones, la Autoridad de Protección de Datos Personales emitirá resolución motivada, en la que se establezca que la transferencia o comunicación internacional de datos personales cumple niveles adecuados de protección o de garantías adecuadas de protección, conforme a lo establecido en esta ley y su reglamento.

**Artículo 57.- Transferencia o comunicación mediante garantías adecuadas.-** En caso de realizar una transferencia internacional de datos a un país, organización o territorio económico internacional que no haya sido calificado por la Autoridad de Protección de Datos de tener un nivel adecuado de protección, se podrá realizar la referida transferencia internacional siempre que el responsable o encargado del tratamiento de datos personales ofrezca garantías adecuadas para el titular, para lo cual se deberá observar lo siguiente:

a. Garantizar el cumplimiento de principios, derechos y obligaciones en el tratamiento de datos personales en un estándar igual o mayor a la normativa ecuatoriana vigente.

b. Efectiva tutela del derecho a la protección de datos personales, a través de la disponibilidad permanente de acciones administrativas o judiciales; y,

c. El derecho a solicitar la reparación integral, de ser el caso.

Para que ello ocurra, la transferencia internacional de datos personales se sustentará en un instrumento jurídico que contemple los estándares antes determinados, así como aquellos que establezca la Autoridad de Protección de Datos Personales, el mismo que deberá ser vinculante.

**Artículo 58. Normas corporativas vinculantes.-** Los responsables o encargados del tratamiento de datos personales podrán presentar a la Autoridad de Protección de Datos Personales, normas corporativas vinculantes, específicas y aplicadas al ámbito de su actividad, las cuales deberán cumplir las siguientes condiciones:

1. Será de obligatorio cumplimiento para el responsable del tratamiento y para la empresa a la que eventualmente transfieran datos personales.

2. Brindar a los titulares los mecanismos adecuados para el ejercicio de sus derechos relacionados al tratamiento de sus datos personales observando las disposiciones de la presente ley;

3. Incluir una enunciación detallada de las empresas filiales que, además del responsable del tratamiento, pertenecen al mismo grupo empresarial. Además, se incluirá la estructura y los datos del contacto del grupo empresarial o joint venture, dedicadas a una actividad económica conjunta y de cada uno de sus miembros.

4. Incluir el detalle de las empresas encargadas del tratamiento de datos personales, las categorías de datos personales a ser utilizados, así como el tipo de tratamiento a realizarse y su finalidad;

5. Observar en su contenido todas las disposiciones de la presente ley referentes a principios de tratamiento de datos personales, medidas de seguridad de datos, requisitos respecto a transferencia o comunicación internacional y transferencia o comunicación ulterior a organismos no sujetos a normas corporativas vinculantes;

6. Contener la aceptación por parte del responsable o del encargado del tratamiento de los datos personales, o de cualquier miembro de su grupo empresarial sobre su responsabilidad por cualquier violación de las normas corporativas vinculantes. El responsable o encargado del tratamiento de datos personales no será responsable si demuestra que el acto que originó la violación no le es imputable;

7. Incluir los mecanismos en que se facilita al titular la información clara y completa, respecto a las normas corporativas vinculantes;

8. Incluir las funciones de todo delegado de protección de datos designado de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o del joint venture dedicadas a una actividad económica conjunta bajo un mismo control así como los mecanismos y procesos de supervisión y tramitación de reclamaciones;

9. Enunciar de forma detallada los mecanismos establecidos en el grupo empresarial o empresas afiliadas que permitan al titular verificar efectivamente el cumplimiento de las normas corporativas vinculantes. Entre estos mecanismos se incluirán auditorías de protección de datos, y aquellos métodos técnicos que brinden acciones correctivas para proteger los derechos del titular. Los resultados de las auditorías serán comunicadas al delegado de protección de datos designado de conformidad con la presente ley, o cualquier otra entidad o persona encargada del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o empresas afiliadas dedicadas a una actividad económica conjunta y al Directorio de la empresa que controla un grupo empresarial, y a disposición de la Autoridad de protección de datos personales;

10. Incluir los mecanismos para cooperar de forma coordinada con la autoridad de protección de datos personales y el responsable del tratamiento de los datos personales; y,

11. Incluir la declaración y compromiso del responsable del tratamiento de los datos personales de promover la protección de datos personales entre sus empleados con formación continua.

La Autoridad de Protección de Datos Personales definirá el formato y los procedimientos para la transferencia o comunicación de datos realizada por parte de los responsables, los encargados y las autoridades de control en lo relativo a la aplicación de las normas corporativas vinculantes a las que se refiere este artículo.

Cualquier cambio a ser realizado a estas normas deberá ser notificado a la autoridad de protección de datos personales y al titular conforme a los mecanismos señalados por el responsable de tratamiento en su solicitud.

**Artículo 59.- Autorización para transferencia internacional.-** Para todos aquellos casos no contemplados en los artículos precedentes, en los que se pretenda realizar una transferencia internacional de datos personales, se requerirá la autorización de la Autoridad de Protección de Datos, para lo cual, se deberá garantizar documentadamente el cumplimiento de la normativa vigente sobre protección de datos de carácter personal, según lo determinado en el Reglamento de aplicación a la presente Ley.

Sin perjuicio de lo anterior, la información sobre transferencias internacionales de datos personales deberá ser registradas previamente en el Registro Nacional de

Protección de Datos Personales por parte del responsable del tratamiento o, en su caso, del encargado, según el procedimiento establecido en el Reglamento de aplicación a la presente Ley.

**Artículo 60. Casos excepcionales de transferencias o comunicaciones internacionales.**- Sin perjuicio de lo establecido en los artículos precedentes se podrá realizar transferencias o comunicaciones internacionales de datos personales, en los siguientes casos:

1. Cuando los datos personales sean requeridos para el cumplimiento de competencias institucionales, de conformidad con la normativa aplicable;

2. Cuando el titular haya otorgado su consentimiento explícito a la transferencia o comunicación propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias o comunicaciones internacionales, debido a la ausencia de una resolución de nivel adecuado de protección y de garantías adecuadas.

3. Cuando la transferencia internacional tenga como finalidad el cumplimiento de una obligación legal o regulatoria;

4. Cuando la transferencia internacional de datos personales sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento de datos personales, o para la ejecución de medidas de carácter precontractual adoptadas a solicitud del titular;

5. Cuando la transferencia sea necesaria por razones de interés público.

6. Cuando la transferencia internacional sea necesaria para la colaboración judicial internacional.

7. Cuando la transferencia internacional sea necesaria para la cooperación dentro de la investigación de infracciones.

8. Cuando la transferencia internacional es necesaria para el cumplimiento de compromisos adquiridos en procesos de cooperación internacional entre Estados;

9. Cuando se realicen transferencias de datos en operaciones bancarias y bursátiles.

10. Cuando la transferencia internacional de datos personales sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones, acciones administrativas o jurisdiccionales y recursos; y,

11. Cuando la transferencia internacional de datos personales sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.

**Artículo 61.- Control continuo.-** La Autoridad de Protección de Datos Personales en acciones conjuntas con la academia, realizará reportes continuos sobre la realidad internacional en materia de protección de datos personales. Dichos estudios servirán como elemento de control continuo del nivel adecuado de protección de datos personales de los países u organizaciones que ostenten tal reconocimiento.

En caso de detectarse que un país u organización ya no cumple con un nivel adecuado de protección conforme los principios, derechos y obligaciones desarrollados en la presente Ley, la Autoridad de Protección de Datos Personales procederá a emitir la correspondiente resolución de no adecuación, a partir de la cual no procederán transferencias de datos personales, salvo que operen otros mecanismos de transferencia conforme lo dispuesto en el presente capítulo.

La Autoridad de Protección de Datos Personales publicará en cualquier medio, de forma permanente y debidamente la lista de países, organizaciones, empresas o grupos económicos que garanticen niveles adecuados de protección de datos personales

## CAPÍTULO X

## DE LOS REQUERIMIENTOS DIRECTOS Y DE LA GESTIÓN DEL PROCEDIMIENTO ADMINISTRATIVO

**Artículo 62.- Requerimiento directo del titular del dato de carácter personal al responsable del tratamiento.-** El titular podrá en cualquier momento, de forma gratuita, por medios físicos o digitales puestos a su disposición por parte del responsable del tratamiento de los datos personales, presentar requerimientos, peticiones, quejas o reclamaciones directamente al responsable del tratamiento, relacionadas con el ejercicio de sus derechos, la aplicación de principios y el cumplimiento de obligaciones por parte del responsable del tratamiento, que tengan relación con él.

Presentado el requerimiento ante el responsable este contará con un término de diez (10) días para contestar afirmativa o negativamente, notificar y ejecutar lo que corresponda.

**Artículo 63.- Actuaciones previas.-** La Autoridad de Protección de Datos Personales podrá iniciar, de oficio o a petición del titular, actuaciones previas con el fin de conocer las circunstancias del caso concreto o la conveniencia o no de iniciar el procedimiento, para lo cual se estará conforme a las disposiciones del Código Orgánico Administrativo.

**Artículo 64.- Procedimiento administrativo.-** En el caso de que el responsable del tratamiento no conteste el requerimiento, en el término establecido en la presente ley, o éste fuere negado, el titular podrá presentar el correspondiente reclamo administrativo ante la Autoridad de Protección de Datos Personales, para lo cual se deberá estar conforme al procedimiento establecido en el Código Orgánico Administrativo, la presente ley y demás normativa emitida por la Autoridad de Protección de Datos Personales. Sin perjuicio, el titular podrá presentar acciones civiles, penales o constitucionales de las que se crea asistido.

## CAPÍTULO XI

## MEDIDAS CORRECTIVAS, INFRACCIONES Y RÉGIMEN SANCIONATORIO

**Artículo 65.- Medidas correctivas.-** En caso de incumplimiento de las disposiciones previstas en la presente Ley, su reglamento, directrices y lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia, o transgresión a los derechos y principios que componen el derecho a la protección de datos personales, la Autoridad de Protección de Datos Personales dictará medidas correctivas con el objeto de evitar que se siga cometiendo la infracción y que la conducta se produzca nuevamente, sin perjuicio de la aplicación de las correspondientes sanciones administrativas.

Las medidas correctivas podrán consistir, entre otras, en:

1) El cese del tratamiento, bajo determinadas condiciones o plazos;

2) La eliminación de los datos; y

3) La imposicion de medidas técnicas, jurídicas, organizativas o administrativas a garantizar un tratamiento adecuado de datos personales.

La Autoridad de Protección de Datos Personales, en el marco de esta Ley, dictará, para cada caso, las medidas correctivas, previo informe de la unidad técnica competente, que permitan corregir, revertir o eliminar las conductas contrarias a la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia.

**Artículo 66.- Aplicación de medidas correctivas.-** La Autoridad de Protección de Datos Personales, en el marco de esta ley, previo informe de la unidad técnica competente, aplicará para cada caso las medidas correctivas citadas en el artículo anterior, que permitan corregir, revertir o eliminar las conductas contrarias a la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Para la aplicación de las medidas correctivas se seguirán las siguientes reglas:

1. En el caso de que los responsables, encargados de tratamiento de datos personales y organismos de certificación y de ser el caso, a terceros, se encuentran incursos en el presunto cometimiento de una infracción leve y estos consten dentro del Registro Único de responsables y encargados incumplidos; la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio, haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida; y,

2. En el caso de que los responsables, encargados del tratamiento de datos personales y organismos de certificación, se encuentren incursos en el presunto cometimiento de una infracción grave; la Autoridad de Protección de Datos Personales; aplicará en primera instancia medidas correctivas. Si las medidas correctivas fueren cumplidas de forma tardía, parcial o defectuosa, la Autoridad de Protección de Datos Personales, aplicará las sanciones que corresponden a las infracciones graves, activando para el efecto el procedimiento administrativo sancionatorio y haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida; y,

3. En el caso de que los responsables, encargados del tratamiento de datos personales y organismos de certificación, se encuentren incursos en el presunto cometimiento de una infracción muy grave, la Autoridad de Protección de Datos

Personales activará directamente el procedimiento administrativo sancionatorio haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida.

**Sección 1a**

**De las infracciones del Responsable de protección de datos**

**Artículo 67.- Infracciones leves del Responsable de protección de datos.-** Se consideran infracciones leves las siguientes:

1. No tramitar, tramitar fuera del término previsto o negar injustificadamente las peticiones o quejas realizadas por el titular;

2. No implementar protección de datos desde el diseño y por defecto;

3. No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales;

4. Elegir un encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales;

5. Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.

**Artículo 68.- Infracciones graves del Responsable de protección de datos.-** Se consideran infracciones graves las siguientes:

1) No implementar medidas administrativas, técnicas y físicas, organizativas y jurídicas, a fin de garantizar el tratamiento de datos personales que realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia;

2) Utilizar información o datos para fines distintos a los declarados;

3) Ceder o comunicar datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente ley y su reglamento, directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia,

4) No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales las particularidades del tratamiento y de las partes involucradas;

5) No realizar evaluaciones de impacto al tratamiento de datos en los casos en que era necesario realizarlas;

6) No implementar medidas técnicas organizativas o de cualquier índole, necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones a la seguridad de datos personales que hayan sido identificadas;

7) No notificar a la Autoridad de Protección de Datos Personales y al titular, de vulneraciones a la seguridad y protección de datos personales, cuando afecte los derechos fundamentales y libertades individuales de los titulares;

8) No notificar a la Autoridad de Protección de Datos Personales del titular las vulneraciones de seguridad y protección de datos personales, cuando exista afectación a los derechos fundamentales y libertades individuales de los titulares;

9) No suscribir contratos que incluyen cláusulas de confidencialidad y tratamiento adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;

10) No mantener actualizado el Registro Nacional de protección de datos personales de conformidad a lo dispuesto en la presente ley su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia;

11) No consignar en el Registro Nacional de Protección de Datos Personales lo dispuesto en la presente ley y su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia;

12) No designar al delegado de protección de datos personales cuando corresponda;

13) No permitir y no contribuir a la realización de auditorías o inspecciones por parte del auditor acreditado por la Autoridad de Protección de Datos Personales; y,

14) Incumplir las medidas correctivas o cumplir de forma tardía, parcial o defectuosa, siempre y cuando hubiere precedido por dicha causa la aplicación de una sanción por infracción leve, o incurrir de forma reiterada en faltas leves.

**Sección 2a**

**De las infracciones del Encargado de protección de datos**

**Artículo 69.- Infracciones leves del Encargado de protección de datos.-** Se consideran infracciones leves las siguientes:

1) No colaborar con el responsable del tratamiento datos personales, para que este cumpla con su obligación de atender solicitudes que tengan por objeto el ejercicio de los derechos del titular frente al tratamiento de sus datos personales;

2) No facilitar el acceso al responsable del tratamiento de datos personales a toda la información referente al cumplimiento de las obligaciones establecidas en la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;

3) No permitir o no contribuir a la realización de auditorías o inspecciones, por parte del responsable del tratamiento de datos personales o de otro auditor autorizado por la Autoridad de Protección de Datos Personales; y,

4) Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.

**Artículo 70.- Infracciones graves del Encargado de protección de datos.-** Se consideran infracciones graves las siguientes:

1) Realizar tratamientos de datos personales sin observar los principios y derechos desarrollados en la presente Ley y su reglamento, directrices y lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia;

2) No tratar datos personales de conformidad con lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales inclusive en lo que respecta a la transferencia o comunicación internacional;

3) No suscribir contratos que contengan cláusulas de confidencialidad y tratamiento adecuado de datos personales con el personal a cargo del tratamiento de datos personales o quien tenga conocimiento de los datos personales;

4) No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;

5) No implementar medidas preventivas y correctivas en la seguridad de los datos personales a fin de evitar vulneraciones;

6) No suprimir los datos personales transferidos o comunicados al responsable del tratamiento de los datos personales, una vez haya culminado su encargo;

7) Proceder a la comunicación de datos personales sin cumplir con los requisitos y procedimientos establecidos en la presente ley, su reglamento directrices lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia;

8) Incumplir las medidas correctivas o cumplirlas de forma tardía parcial o defectuosa, siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve; y,

9) No notificar al responsable del tratamiento de datos personales sobre cualquier vulneración de la seguridad de datos personales conforme dispone esta ley o hacerlo con retraso injustificado.

**Artículo 71.- Sanciones por infracciones leves.-** La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción leve, según las siguientes reglas:

1. Servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones leves establecidas en la presente ley, serán sancionados con una multa de uno (1) a diez (10) salarios básicos unificados del trabajador en general, sin perjuicio de la responsabilidad extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente;

2. Si el responsable o el encargado del tratamiento de datos personales o de ser el caso un tercero es una entidad de derecho privado o una empresa pública, se aplicará una multa de entre el 0.1% y el 0.7% calculada sobre su volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la

imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad, para lo cual deberá verificar los siguientes presupuestos:

a) La intencionalidad, misma que se establecerá en función a la conducta del infractor;

b) Reiteración de la infracción, es decir cuando el responsable, el encargado del tratamiento de datos personales o de ser el caso un tercero, hubiese sido previamente sancionado por dos o más infracciones precedentes, que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;

c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,

d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

**Artículo 72.- Sanciones por infracciones graves.-** La Autoridad de Protección de Datos Personales impondrán las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción grave, conforme a los presupuestos establecidos en el presente Capítulo:

Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente ley serán sancionados con una multa de entre 10 a 20 salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente;

1) Si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero, es una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales

establecerá la multa aplicable en función del principio de proporcionalidad, para lo cual deberá verificar los siguientes presupuestos:

a) La intencionalidad, misma que se establecerá en función a la conducta del infractor;

b) Reiteración de la infracción, es decir, cuando el responsable, encargado del tratamiento de datos personales o de ser el caso, de un tercero hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;

c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,

d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

En el caso de que el responsable, encargado del tratamiento de datos personales a un tercero de ser el caso; sea una organización sin domicilio ni representación jurídica en el territorio ecuatoriano, se deberá notificar de la resolución con la cual se establezca la infracción cometida la Autoridad de Protección de Datos Personales, o quien hiciera sus veces, del lugar en donde dicha organización tiene su domicilio principal, a fin de que sea dicho organismo quien sustancia las acciones o procedimientos destinados al cumplimiento de las medidas correctivas y sanciones a las que hubiere lugar.

**Artículo 73.- Volumen de negocio.-** A efectos del régimen sancionatorio de la presente ley, se entiende por volumen de negocio, a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica.

**Artículo 74.- Medidas provisionales o cautelares.-** La Autoridad de Protección de Datos Personales podrá aplicar medidas provisionales de protección o medidas cautelares contempladas en la norma procedimental administrativa.

## CAPÍTULO XII

## AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

**Artículo 75.- Autoridad de protección de datos personales.-** La Autoridad de Protección de Datos Personales podrá iniciar, de oficio o a petición del titular, actuaciones previas con el fin de conocer las circunstancias del caso concreto o la conveniencia o no de iniciar el procedimiento, para lo cual se estará conforme a las disposiciones del Código Orgánico Administrativo.

**Artículo 76.- Funciones atribuciones y facultades.-** La Autoridad de Protección de Datos Personales es el órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley y en su reglamento de aplicación, para lo cual le corresponde las siguientes funciones, atribuciones y facultades:

1) Ejercer la supervisión, control y evaluación de las actividades efectuadas por el responsable y encargado del tratamiento de datos personales;

2) Ejercer la potestad sancionadora respecto de responsables, delegados, encargados y terceros, conforme a lo establecido en la presente Ley;

3) Conocer, sustanciar y resolver los reclamos interpuestos por el titular o aquellos iniciados de oficio, así como aplicar las sanciones correspondientes;

4) Realizar o delegar auditorías técnicas al tratamiento de datos personales;

5) Emitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y la garantía del ejercicio del derecho a la protección de datos personales;

6) Crear, dirigir y administrar el Registro Nacional de Protección de Datos Personales, así como coordinar las acciones necesarias con entidades del sector público y privado para su efectivo funcionamiento;

7) Promover una coordinación adecuada y eficaz con los encargados de la rendición de cuentas y participar en iniciativas internacionales y regionales para la protección de la protección de los datos personales;

8) Dictar las cláusulas estándar de protección de datos, así como verificar el contenido de las cláusulas o garantías adicionales o específicas;

9) Atender consultas en materia de protección de datos personales;

10) Ejercer el control y emitir las resoluciones de autorización para la transferencia internacional de datos;

11) Ejercer la representación internacional en materia de protección de datos personales;

12) Emitir directrices para el diseño y contenido de la política de tratamiento de datos personales;

13) Establecer directrices para el análisis evaluación y selección de medidas de seguridad de los datos personales,

14) Llevar un registro estadístico sobre vulneraciones a la seguridad de datos personales e identificar posibles medidas de seguridad para cada una de ellas;

15) Publicar periódicamente una guía de la normativa relativa a la protección de datos personales;

16) Promover e incentivar el ejercicio del derecho a la protección de datos personales, así como la concientización en las personas y la comprensión de los riesgos, normas, garantías y derechos, en relación con el tratamiento y uso de sus datos personales, con especial énfasis en actividades dirigidas a grupos de atención prioritaria tales como niñas niños y adolescentes;

17) Controlar y supervisar el ejercicio del derecho a la protección de datos personales dentro del tratamiento de datos llevado a cabo a través del Sistema Nacional de Registros Públicos; y,

18) Las demás atribuciones establecidas en la normativa vigente.

**Artículo 77.- Del titular de la Autoridad de Protección de Datos.-** El Superintendente de Protección de Datos será designado de acuerdo a lo establecido en la Constitución de la República, de la terna que remita la Presidente o Presidente de la República, siguiendo criterios de especialidad y méritos; se sujetará a escrutinio público y derecho de impugnación ciudadana.

El Superintendente de Protección de Datos deberá ser un profesional del Derecho, de Sistemas de Información, de Comunicación o de Tecnologías, con título de

cuarto nivel y experiencia de al menos 10 años con áreas afines a la materia objeto de regulación de esta ley.

Ejercerá sus funciones por un periodo de 5 años y únicamente cesará en sus funciones por las causales establecidas en la ley que regula el servicio público que le sean aplicables o por destitución, luego de enjuiciamiento político realizado por la Asamblea Nacional.

## DISPOSICIONES GENERALES

**PRIMERA.-** En lo dispuesto al procedimiento administrativo se estará a lo previsto en el Código Orgánico Administrativo.

**SEGUNDA.-** En el ámbito del derecho de acceso a la información pública son aplicables las disposiciones de las leyes de la materia.

**TERCERA.-** En el ámbito de los datos personales registrables, son aplicables las disposiciones de las leyes de la materia.

**CUARTA.-** La Autoridad de Protección de Datos Personales será responsable de coordinar las acciones necesarias con entidades del sector público y privado para el efectivo funcionamiento del Registro Nacional de Protección de Datos Personales.

**QUINTA.-** La Autoridad de Protección de Datos Personales será responsable de presentar informes anuales de evaluación y revisión de la presente Ley, a la ciudadanía.

**SEXTA.-** Créase el Registro Único de Responsables y Encargados Incumplidos, en el cual se llevará un registro de los Responsables y Encargados del Tratamiento de Datos Personales, que hayan incurrido en una de las infracciones establecidas en la presente Ley; mismo que tendrá fines sociales, estadísticos, preventivos y de capacitación, cuyo funcionamiento estará establecido en el Reglamento de la Ley de Protección de Datos Personales.

**SÉPTIMA.-** El ejercicio de los derechos reconocidos en la presente norma podrá ser exigido por el titular independientemente de la entrada en vigor del régimen sancionatorio.

**OCTAVA.-** Ninguna entidad pública o privada, podrá cobrar valores por servicios de entrega de información sustentada en datos del solicitante de los mismos.

**NOVENA.**- Se procurará que en lo referente a los pueblos y nacionalidades indígenas, el tratamiento de sus datos personales sea en sus idiomas y lenguas ancestrales.

## DISPOSICIONES TRANSITORIAS

**PRIMERA.**- Las disposiciones relacionadas con las medidas correctivas y el régimen sancionatorio entrarán en vigencia en dos años contados a partir de la publicación de esta ley en el Registro Oficial, en el transcurso de este tiempo los responsables y encargados del tratamiento de datos personales se adecuarán a los preceptos establecidos dentro de esas disposiciones, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales. El resto de disposiciones establecidas en esta ley entrarán en vigencia conforme se establece en la Disposición Final de esta Ley.

**SEGUNDA.**- Todo tratamiento realizado previo a la entrada en vigencia de la presente Ley deberá adecuarse a lo previsto en la presente norma dentro del plazo de dos años contados a partir de su publicación en el Registro Oficial.

El incumplimiento de la presente disposición dará lugar a la aplicación del régimen sancionatorio establecido en esta Ley.

**TERCERA.**- Los responsables y encargados del tratamiento de datos personales que hayan implementado los preceptos recogidos dentro de esta Ley antes de plazo señalado en la Disposición Transitoria Primera obtendrán un reconocimiento por buenas prácticas por parte de la Autoridad de Protección de Datos Personales.

**CUARTA.**- La transferencia internacional de datos personales que hubiere sido realizada antes de la entrada en vigencia de la presente Ley será legítima, sin perjuicio de que el responsable del tratamiento de datos personales deba aplicar lo dispuesto en esta norma para acreditar su responsabilidad proactiva y demostrada.

El responsable de tratamiento deberá adecuar la transferencia internacional de datos personales a la presente norma en un plazo no mayor de dos años contados a partir de la publicación de la presente norma en el Registro Oficial.

El incumplimiento de la presente disposición dará lugar a la aplicación del régimen sancionatorio establecido en esta Ley.

## DISPOSICIONES REFORMATORIAS

**PRIMERA.**- De la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Suplemento del Registro Oficial 557 del 17 de abril de 2002:

1. Suprímese las definiciones de intimidad, datos personales, datos personales autorizados del glosario de términos establecido en la Disposición General Novena.

**SEGUNDA.**- En la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicada en el suplemento del Registro Oficial 162 del 31 de marzo del 2010:

1.- Sustitúyese:

a) El término Dirección Nacional de Registro de Datos Públicos por Dirección Nacional de Registros Públicos;

b) El término Sistema Nacional de Registro de Datos Públicos por Sistema Nacional de Registros Públicos;

c) El término Registro de Datos Públicos por Registros Públicos;

d) El término datos de carácter personal por datos personales;

e) El término datos públicos registrales por la expresión datos públicos y datos personales registrables;

f) El artículo 6, por el siguiente: "Art. 6.- Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal. El acceso a estos datos, solo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales.

Al amparo de esta Ley, para acceder a la información sobre el patrimonio de las personas cualquier solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará del mismo y consignar sus datos básicos de identidad, tales como nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo

reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el titular de la información pueda ejercer.

La Directora o Director Nacional de Registros Públicos, definirá los demás datos que integran el sistema nacional y el tipo de reserva y accesibilidad.

2.- Incorpórase:

a) En el artículo 31 referente a las atribuciones y facultades de la Dirección Nacional de Registro Públicos antes del numeral 14 lo siguiente:

"14. Controlar y supervisar que las entidades pertenecientes al Sistema Nacional de Registros Públicos incorporen mecanismos de protección de datos personales, así como dar cumplimiento a las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación y demás normativa que la Autoridad de Protección de Datos Personales dicte para el efecto:

15. Tratar datos procedentes del Sistema Nacional de Registros Públicos o de cualquier otra fuente, para realizar procesos de analítica de datos, con el objeto de prestar servicios al sector público, al sector privado y a personas en general, así como generar productos, reportes, informes o estudios, entre otros. Se utilizarán medidas adecuadas que garanticen el derecho a la protección de datos personales y su uso en todas las etapas del tratamiento, como por ejemplo, técnicas de disociación de datos, y,"

3.- Suprímese del numeral 13 del artículo 31 lo siguiente: "y";

4.- Reenumerar el numeral 14 del artículo 31 por numeral "16".

**TERCERA.**- En el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación publicado en el suplemento del Registro Oficial 899 del 09 de diciembre de 2016, sustitúyase la palabra confidencialidad por Protección en el numeral 5 del artículo 67.

**CUARTA.**- En la Ley Orgánica de Telecomunicaciones, publicada en el tercer suplemento del Registro Oficial 439 del 18 de febrero de 2015:

1.- Suprímese:

a) El inciso segundo, tercer y cuarto del artículo 79;

b) En el primer inciso del artículo 83 lo siguiente "(...) y seguridad de datos personales (...)"; y,

c) En el inciso primero del artículo 85 lo siguiente "(...) como de seguridad de datos personal (...)"

2.- Sustitúyese:

a) El artículo 78 por el siguiente:

"Art. 78.- Seguridad de los Datos Personales.- Las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas, organizativas y de cualquier otra índole adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos personales de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales."

b) El artículo 81 por el siguiente:

"Art. 81.- Guías telefónicas o de abonados en general.- Los abonados, clientes o usuarios tienen el derecho a no figurar en guías telefónicas o de abonados. Deberán ser informados, de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales, de sus derechos con respecto a la utilización de sus datos personales en las guías telefónicas o de abonados y, en particular, sobre el fin o los fines de dichas guías, así como sobre el derecho que tienen, en forma gratuita, a no ser incluidos, en tales guías."

c) El artículo 82 por el siguiente:

"Art. 82.- Uso comercial de datos personales.- Las y los prestadores de servicios no podrán usar datos personales, información del uso del servicio, información de tráfico o el patrón de consumo de sus abonados, clientes o usuarios para la promoción comercial de servicios o productos, a menos que el abonado o usuario al que se refieran los datos o tal información, haya dado su consentimiento conforme lo establecido en la Ley Orgánica de Protección de Datos Personales. Los usuarios o abonados dispondrán de la posibilidad clara y fácil de retirar su consentimiento para el uso de sus datos y de la información antes indicada. Tal consentimiento deberá especificar los datos personales o información cuyo uso se autorizan, el tiempo y su objetivo específico.

Sin contar con tal consentimiento y con las mismas características, las y los prestadores de servicios de telecomunicaciones no podrán comercializar, ceder o

transferir a terceros los datos personales de sus usuarios, clientes o abonados. Igual requisito se aplicará para la información del uso del servicio, información de tráfico o del patrón de consumo de sus usuarios, clientes y abonados."

d) El artículo 83 por el siguiente:

"Art. 83 - Control técnico.- Cuando para la realización de las tareas de control técnico, ya sea para verificar el adecuado uso del espectro radioeléctrico, la correcta prestación de los servicios de telecomunicaciones, el apropiado uso y operación de redes de telecomunicaciones o para comprobar las medidas implementadas para garantizar el secreto de las comunicaciones y seguridad de datos personales, sea necesaria la utilización de equipos, infraestructuras e instalaciones que puedan vulnerar la seguridad e integridad de las redes. La Agencia de Regulación y Control de las Telecomunicaciones deberá diseñar y establecer procedimientos que reduzcan al mínimo el riesgo de afectar los contenidos de las comunicaciones.

Cuando, como consecuencia de los controles técnicos efectuados, quede constancia de los contenidos, se deberá coordinar con la Autoridad de Protección de Datos Personales para que:

a) Los soportes en los que éstos aparezcan no sean ni almacenados ni divulgados; y,

b) Los soportes sean inmediatamente destruidos y desechados.

Si se evidencia un tratamiento ilegítimo o ilícito de datos personales, se aplicará lo dispuesto en la Ley Orgánica de Protección de Datos Personales."

## DISPOSICIONES DEROGATORIAS

**PRIMERA.-** Derógase el artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el suplemento del Registro Oficial 557 del 17 de abril de 2002.

**SEGUNDA.-** Derógase los artículos 80 y 84 de la Ley Orgánica de Telecomunicaciones, publicada en el tercer suplemento del Registro Oficial 439 del 18 de febrero de 2015.

**TERCERA.-** Derógase el artículo 5 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicada en el Suplemento del Registro Oficial 162 de 31 de marzo de 2010.

**CUARTA.-** Quedan así mismo derogadas todas aquellas disposiciones de igual o menor jerarquía que se contrapongan con la presente Ley Orgánica.

**DISPOSICIÓN FINAL**

La presente Ley entrará en vigencia una vez publicada en el Registro Oficial.

Dado y suscrito, a los diez días del mes de mayo del año dos mil veintiuno.

**ING. CÉSAR LITARDO CAICEDO**
Presidente

**DR. JAVIER RUBIO DUQUE.**
Secretario General

PALACIO NACIONAL, DISTRITO METROPOLITANO DE QUITO, A VEINTIUNO DE MAYO DE DOS MIL VEINTIUNO.

SANCIONASE Y PROMULGASE

Lenín Moreno Garcés
PRESIDENTE CONSTITUCIONAL DE LA REPUBLICA

Es fiel copia del original.- Lo Certifico.
Quito, 21 de mayo de 2021

PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR
Secretaría General Jurídica

Dra. Johana Pesántez Benítez
SECRETARIA GENERAL JURÍDICA
PRESIDENCIA DE LA REPÚBLICA


Ing. Hugo Del Pozo Barrezueta
DIRECTOR

Quito:
Calle Mañosca 201 y Av. 10 de Agosto
Telf.: 3941-800
Exts.: 3131 - 3134

www.registroficial.gob.ec

El Pleno de la Corte Constitucional mediante Resolución Administrativa No. 010-AD-CC-2019, resolvió la gratuidad de la publicación virtual del Registro Oficial y sus productos, así como la eliminación de su publicación en sustrato papel, como un derecho de acceso gratuito de la información a la ciudadanía ecuatoriana.

*"Al servicio del país desde el 1º de julio de 1895"*

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

**MEMORANDO No. PAN-CLC-2019-** 0184

**DE:** **CÉSAR LITARDO CAICEDO**
Presidente de la Asamblea Nacional

**PARA:** **JOHN DE MORA MONCAYO**
Prosecretario General Temporal

**ASUNTO:** Difundir Proyecto

**FECHA:** Quito D.M, 19 SEP 2019

---

Según lo dispuesto en el Art. 55 de la Ley Orgánica de la Función Legislativa, envío el **"PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES"**, remitido por el Presidente Constitucional de la República, Lenín Moreno Garcés, a través del oficio No. T.514-SGJ-19-0740 de 19 de septiembre de 2019, con número de trámite 379637, a fin de que sea difundido a las/los asambleístas y a la ciudadanía a través del portal Web y se remita al Consejo de Administración Legislativa (CAL), para el trámite correspondiente.

Atentamente,

**CÉSAR LITARDO CAICEDO**
Presidente de la Asamblea Nacional

tr. 379637
jda.

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

# Trámite 379637
Código validación QNAH1RXUON
Tipo de documento OFICIO
Fecha recepción 19-sep-2019 14:16
Numeración documento t.514-sgj-19-0740
Fecha oficio 19-sep-2019
Remitente MORENO GARCES LENIN
Razón social PRESIDENCIA DE LA REPUBLICA DEL ECUADOR
Revise el estado de su trámite en http://tramites.asambleanacional.gob.ec/EstadoTramite/

Oficio 1 foja
Anexo: 50 fojas

# PRESIDENCIA DE LA REPÚBLICA

Oficio No. T.514-SGJ-19-0740

Quito, 19 de septiembre de 2019

Señor Ingeniero
César Litardo Caicedo
**PRESIDENTE DE LA ASAMBLEA NACIONAL**
En su despacho

De mi consideración:

De conformidad con el numeral 2 del Artículo 134 de la Constitución de la República y el numeral 2 del Artículo 54 de la Ley Orgánica de la Función Legislativa, adjunto le remito a usted y, por su intermedio, a la Asamblea Nacional, el proyecto de **LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES**, así como la correspondiente exposición de motivos, para su conocimiento, discusión y aprobación.

Con sentimientos de distinguida consideración y estima.

Atentamente,

Lenín Moreno Garcés
**PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA**

**Anexo lo indicado**

# PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR

## LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

### Exposición de Motivos:

Es de conocimiento general el espíritu cambiante de la sociedad en que vivimos, las nuevas tendencias y comportamientos componen un sinfín de mecanismos que enmarcan caminos y definen horizontes El individuo en sí mismo pertenece a un conglobado de oportunidades que siembra libertades, pero no siempre las materializa, esto en virtud de elementos que ajenos a los fines se apropia de ellos y los modifican.

El legislador en esta posición y en términos aristotélicos vendría a ser la justicia animada, en donde el justo medio de un todo revelará una sociedad fructífera, que no esté viciada por extremos equiparables a una inequidad que dista de lo justo que en sí mismo debe ser permanente y acceder a todos los espacios para adjudicarse como tal.

En este contexto es imperante mencionar que el espacio en el que actualmente el individuo se desarrolla no se limita a sus expectativas, sino más bien, en sintonía con la evolución previamente mencionada, el sujeto es símbolo de conservación, labra estrategias que le permiten afianzarse a un terreno sólido y en el camino sobrevivir ante la vulneración de sus libertades, ya que como es conocido, todo aquel mecanismo que las genere será el mismo que las limitará

Trasladándolo al escenario actual, la colectividad ha experimentado cambios que por su irrevocable importancia han dejado precedentes en la historia, esto es por ejemplo un relativismo ideológico, nuevas formas de agrupación familiar, aumento en la esperanza de vida y en paralelo disminución de la tasa de natalidad y en particular la omnipresencia de la tecnología.

Es así que el individuo aun víctima de las dificultades que con ello advienen, recolecta los aspectos positivos y disfruta de los avances en todo ámbito posible, en el caso puntual, la región digital que de la mano con el perfeccionamiento tecnológico extienden las posibilidades de un nuevo mundo, colaborando así no solo con la efectivización de procesos sino también con el desarrollo económico, facilitando el vivir cotidiano creando redes de distribución de la información y generando en función a ello réditos económicos.

Es de admitir que, las personas se desenvuelven en una sociedad altamente conectada, esto permite que la provisión de distintos servicios y la comunicación, se realicen desde cualquier parte del mundo y en tiempo real. Las tecnologías de la información y comunicación (TIC) han impactado sustancialmente en la vida de las personas, tanto es así, que se han convertido en herramientas y procesos indispensables e ineludibles para la satisfacción de necesidades básicas de los seres humanos.

Su versatilidad permite que estas logren adaptarse a las necesidades y requerimientos de forma personalizada, es por eso que el ser humano las acopla en todas sus actividades manteniendo con ellas una relación incluso cercana a la dependencia. Como consecuencia de ello se ha generado la omnipresencia de las mismas, en la totalidad de las áreas en las que los individuos se desenvuelven (salud, comercio, educación, migración, cooperación internacional, respeto y garantía de derechos, cultura, entre otros).

Es indudable que las TIC representan un sin número de beneficios que tienen como objetivo mejorar la calidad de vida de los seres humanos, sin embargo, también se ha de reconocer que el mismo potencial ha sido invertido para configurar un espacio lleno de múltiples riesgos para las personas.

Esto en virtud de que los individuos no son conscientes del valor de sus datos; considerando que, usados de manera adecuada, pueden generar una serie de ventajas, no solo para su titular, sino también para los proveedores de bienes o servicios públicos o privados que los procesan; pero cuando se tratan de forma irresponsable o abusiva pueden llegar a afectar gravemente la dignidad e integridad de los seres humanos, es así que, su recopilación, procesamiento y comunicación inadecuada puede significar una vulneración a derechos fundamentales como la vida, la salud, el acceso a servicios públicos, la integridad física, psicológica o sexual, entre muchos otros; lesiones que se han podido evidenciar a nivel mundial y que incluso ya se han familiarizado con la realidad ecuatoriana.

La casi arbitraria libertad con la que se mueve la información acaece desconcierto social por la ausencia de mecanismos de protección que controlen su tratamiento, esto en virtud de que gran parte de esta sujeta datos personales, que utilizados o tratados inadecuadamente pueden, por ejemplo, alterar elecciones presidenciales, determinar quién recibe servicios de salud o alimenticios, ser una herramienta para la delincuencia organizada (trata de personas, narcotráfico o terrorismo). Situaciones que parecen lejanas a nuestra realidad; sin embargo, estas circunstancias se vivencian actualmente incluso en nuestro país, donde se han evidenciado robos, ataques o exposiciones ilegítimas de bases de datos de carácter público o privado, que han generado perjuicios sociales y económicos

En lo que respecta al siglo pasado la relación instituida entre el Estado y el individuo en cuanto a identificación mutua ha sido realmente escasa; el ambiente percibido en tal época se contenía en cajas de información registrada a mano que en virtud del tiempo se volvía frágil, quebrando consigo toda relación existente.

Actualmente el Estado constituye en sí una de las mayores fuentes de información en razón de la posesión de grandes bases de datos necesarias para la consecución de sus fines administrativos, convirtiéndolo en un efectivizador de procesos que atraviesa la delgada línea entre su posición garantista de derechos humanos y la susceptibilidad de vulnerarlos.

A lo largo de la historia, el ser humano ha sido testigo de grandes vulneraciones a la dignidad, debido al procesamiento de información con fines ajenos al interés general, eventos históricos como la Segunda Guerra Mundial no habrían dejado tantas víctimas, si aquellos que abusaron del poder no hubieran tenido en sus manos información que les permitiera aniquilar a millones de personas.

Hito histórico que parece ajeno a nuestra realidad territorial y actual, pero ejemplos como el proyecto SAFARI en la Francia de 1974 o el Plan Cóndor cultivado por los regímenes dictatoriales del Cono Sur que desencadenaron los "Archivos del terror" de Paraguay en 1992, evidencian lo peligroso que puede ser para el ser humano, no ser consciente del valor de su información.

Con la influencia actual de las tecnologías de la información y comunicación, y los procesos de analítica de datos, es cada vez más necesario entender su trascendencia; en el Ecuador, constantemente se suscitan circunstancias de afectación a derechos, debido al tratamiento inadecuado de datos personales, es muy común encontrar noticias que anuncian el robo de bases de datos, la modificación de las mismas para la obtención de beneficios ilegales, incluso, un intento de incidir en su derecho a elegir por la emisión de noticias falsas

Es imperante, denotar que las transgresiones no solo se suscitan en el ámbito público, sino que también ocurren a nivel privado, con mayor frecuencia de la que el individuo percibe; en el Ecuador, cualquier

abonado a servicios móviles, recibe innumerables llamadas para el ofrecimiento de planes celulares, de seguros y tarjetas de crédito, sin conocer cómo empresas con las que nunca han tenido relaciones obtienen su información y que a pesar de su incomodidad no pueden dejar de ser parte de estas redes.

Así mismo, son innumerables las denuncias por el inicio de procesos que tienen el objeto de deudas que en la mayoría de los casos son inexistentes o la denegación de acceso a servicios por criterios sin fundamento y en algunos casos discriminatorio.

Los datos en la actualidad se consideran activos digitales con gran valor económico, incluso equiparable al del dinero; los sujetos se enfrentan a una realidad en donde su información forma parte de un mercado negro, del que nadie habla pero que es innegable

Para enfrentar estas dificultades y aprovechar el potencial de las TIC para el desarrollo sostenible, generar confianza en línea y garantizar las oportunidades que brindan los adelantos tecnológicos, cada uno de los países, sobre la base de su estructura normativa propia, ha optado por desarrollar mecanismos de protección de las personas y sus datos.

Hay pocos Estados que no han desarrollado normativa alguna sobre la materia, o la que tienen es incompleta, dispersa o contradictoria, estos son los que mayor desventaja presentan no solo frente a los riesgos y peligros que trae consigo el manejo de datos personales, sino ante la imposibilidad de usarlos como insumos clave para su desarrollo económico y social, lo cual evidencia la posibilidad real de quedar aún más rezagados.

En ese contexto, es indispensable dar certidumbre a usuarios, empresas, organizaciones y Estados, sobre todo en este momento en el cual la economía mundial se desplaza más hacia un espacio de información masiva, hiperconectada, en tiempo real, de flujo incesante proveniente de internet de las cosas, automatizada con algoritmos de inteligencia artificial cada vez más sofisticados, y de la réplica incesante mediante tecnologías de registros distribuidos. Todo esto, unido a que los datos no tienen fronteras y que las plataformas y servicios son de libre disposición y se almacenan en centros de datos de todo el mundo, obliga a los países a realizar marcos jurídicos compatibles en distintos niveles: nacional, regional y mundial que faciliten el intercambio y al mismo tiempo respeten y protejan los derechos humanos.

Por otro lado, en lo que respecta al contexto internacional, el Consejo de Derechos Humanos de la Asamblea General de Naciones Unidas, en Resolución 28/16 "Profundamente preocupado por los efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones, incluidas la vigilancia y la interceptación extraterritoriales de las comunicaciones y la recopilación de datos personales, en particular cuando se llevan a cabo a gran escala" nombra por primera vez al Relator especial sobre el derecho a la privacidad en la era digital con la finalidad de que, entre otras, presente informes que incluya "observaciones importantes" sobre cómo garantizar este derecho fundamental, así como denuncias sobre posibles violaciones
En el mismo sentido, el 25 de mayo de 2018, entró en vigencia el Reglamento General Europeo de Protección de Datos Personales, su aplicación afecta a todos los países del mundo, ya que únicamente permite e incentiva que países que cuenten con niveles adecuados de protección puedan tratar datos de ciudadanos europeos.

Adicionalmente, es importante mencionar que en el año 2016 se suscribió el Protocolo de Adhesión de Ecuador al Acuerdo Comercial Multipartes con la Unión Europea, con el objetivo de buscar mejores

condiciones para el intercambio de bienes y servicios entre los países miembros de la UE y el Estado ecuatoriano; este acuerdo, sin embargo, se ha visto afectado dado que para el intercambio de bienes o servicios, en la mayoría de los casos, se requiere que exista el flujo transfronterizo de datos personales, y al no tener normativa amparada por un ente controlador especializado en la materia, no le es posible al país ofrecer un nivel adecuado de protección, lo que desalienta el comercio y genera que se prefieran destinos como Colombia, Perú y los demás países suscriptores del acuerdo, que sí cuentan con Ley de Protección de Datos Personales

En virtud de estos antecedentes, y dada la urgencia de legislación especializada que se encargue de regular el tratamiento de datos personales, es necesario contar con una Ley, que salvaguarde los derechos, promueva la actividad económica, comercial, de innovación tecnológica, social, cultural, entre otras y que delimite los parámetros para un tratamiento adecuado en el ámbito público y privado

**PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR**

**EL PLENO**

**CONSIDERANDO:**

Que, el artículo 1 de la Constitución de la República dispone que el "*Estado ecuatoriano es un Estado constitucional de derechos y justicia, social, democrático ( .)*",

Que, los numerales 1, 5 y 8 de la Carta Magna determinan que son deberes primordiales del Estado "*1 Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución y en los instrumentos internacionales, en particular la educación, la salud, la alimentación, la seguridad social y el agua para sus habitantes 5 Planificar el desarrollo nacional, erradicar la pobreza, promover el desarrollo sustentable y la redistribución equitativa de los recursos y la riqueza, para acceder al buen vivir 8 Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción.*";

Que, el numeral 1 del artículo 11 de la Norma Suprema establece que "*Los derechos se podrán ejercer, promover y exigir de forma individual o colectiva ante las autoridades competentes, estas autoridades garantizarán su cumplimiento.*";

Que, el numeral 2 del artículo 11 de la Norma Suprema prescribe que "*Todas las personas son iguales y gozarán de los mismos derechos, deberes y oportunidades* ";

Que, el numeral 3 del artículo 11 de la Constitución de la República preceptúa que "*Los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos serán de directa e inmediata aplicación por y ante cualquier servidora o servidor pública, administrativo o judicial, de oficio o a petición de parte* ";

Que, el numeral 6 del artículo 11 de la Carta Magna determina que "*Todos los principios y derechos son inalienables, indivisibles, interdependientes y de igual jerarquía* ";

Que, el numeral 8 del artículo 11 de la Norma Suprema dispone que "*El contenido de los derechos y garantías establecidos en la Constitución y en los instrumentos internacionales de derechos humanos, no excluirá los demás derechos derivados de la dignidad de las personas, comunidades, pueblos y nacionalidades, que sean necesarios para su pleno desenvolvimiento Será inconstitucional cualquier acción u omisión de carácter regresivo que disminuya, menoscabe o anule injustificadamente el ejercicio de los derechos* ",

Que, el numeral 9 del artículo 11 de la Constitución de la República prescribe que "*El más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución El Estado, sus delegatarios, concesionarios y toda persona que actúe en ejercicio de una potestad pública, estarán obligados a reparar las violaciones a los derechos de los particulares por la falta o deficiencia en la prestación de los servicios públicos, o por las acciones u omisiones de sus funcionarias y funcionarios, y empleadas y empleados públicos en el desempeño de sus cargos* ";

Que, el artículo 16 numerales 1 y 2 de la Carta Magna determina que "*Todas las personas, en forma individual o colectiva, tienen derecho a 1 Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia*

*lengua y con sus propios símbolos 2 El acceso universal a las tecnologías de información y comunicación* ";

Que, el artículo 17 numeral 2 de la Norma Suprema preceptúa que "*El Estado fomentará pluralidad y la diversidad en la comunicación, y al efecto 2 Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de la información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada.*";

Que, el artículo 26 de la Constitución de la República reconoce que "*La educación es un derecho de las personas a lo largo de su vida y un deber inexcusable el Estado Constituye un área prioritaria de la política pública y de la inversión estatal, garantía de la igualdad e inclusión social y condición indispensable para el buen vivir Las personas, las familias y la sociedad tienen el derecho y la responsabilidad de participar en el proceso educativo* ";

Que, el artículo 35 de la Carta Magna establece que "*Las personas adultas mayores, niñas, niños y adolescentes, mujeres embarazadas, personas con discapacidad, personas privadas de libertad y quienes adolezcan de enfermedades catastróficas o de alta complejidad, recibirán atención prioritaria y especializada en los ámbitos públicos y privado La misma atención prioritaria recibirán las personas en situación de riesgo, las víctimas de violencia doméstica y sexual, maltrato infantil, desastres naturales o antropogénicos El Estado prestará especial protección a las personas en condición de doble vulnerabilidad.*",

Que, el artículo 44 de la Norma Suprema dispone que "*El Estado, la sociedad, y la familia promoverán de forma prioritaria el desarrollo integral de las niñas, niños y adolescentes, y asegurarán el ejercicio pleno de sus derechos, se atenderá al principio de su interés superior y sus derechos prevalecerán sobre los de las demás personas Las niñas, niños y adolescentes tendrán derecho a su desarrollo integral, entendido como proceso de crecimiento, maduración y despliegue de su intelecto y de sus capacidades, potencialidades y aspiraciones, en un entorno familiar, escolar, social y comunitario de efectividad y seguridad Este entorno permitirá la satisfacción de sus necesidades sociales, afectivo-emocionales y culturales, con el apoyo de políticas intersectoriales nacionales y locales.*",

Que, el artículo 66 numeral 19 de la Constitución de la República reconoce y garantiza a las personas: "*19 El derecho a la protección de datos carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección La recolección, archivo, procesamiento, distribución o difusión de estos datos personales requerirán la autorización del titular o el mandato de ley* ";

Que, el numeral 25 del artículo 66 de la Norma Suprema prevé que "*Se reconoce y garantizará a las personas 25 El derecho a acceder a bienes y servicios públicos y privados de calidad, con eficiencia, eficacia y buen trato, así como a recibir información adecuada y verás sobre su contenido y características* ";

Que, el numeral 6 del artículo 76 de la Carta Magna determina que "*En todo proceso que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas 6 La Ley establecerá la debida proporcionalidad entre las infracciones y las sanciones penales, administrativas o de otra naturaleza* ";

Que, el artículo 92 de la Norma Suprema prescribe que "*Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez La persona afectada podrá demandar por los perjuicios ocasionados* ",

Que, el numeral 2 del artículo 133 de la Constitución de la República preceptúa que "*Las leyes serán orgánicas y ordinarias* Serán leyes orgánicas. 2. Las que regulan el ejercicio de los derechos y garantías constitucionales.",

Que, el artículo 227 de la Constitución de la República establece que "*La administración pública constituye un servicio a la colectividad que se rige por los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación.*",

Que, el artículo 275 de la Norma Suprema preceptúa que "*El régimen de desarrollo es el conjunto organizado, sostenible y dinámico de los sistemas económicos, políticos, socioculturales y ambientales, que garantizaran la realización del buen vivir, del sumak kawsay El Estado planificará el desarrollo del país para garantizar el ejercicio de los derechos, la consecución de los objetivos del régimen de desarrollo y los principios consagrados en la Constitución La planificación propiciará la equidad social y territorial, promoverá la concertación, y será participativa, descentralizada, desconcentrada y transparente El buen vivir requerirá que las personas, comunidades, pueblos y nacionalidades gocen efectivamente de sus derechos, ejerzan responsabilidades en el marco de la interculturalidad, del respeto a sus diversidades, y de la convivencia armónica con la naturaleza* ";

Que, el numeral 1 y 5 del artículo 276 de la Carta Magna prescriben que "*El régimen de desarrollo tendrá los siguientes objetivos: 1 Mejorar la calidad y esperanza de vida, y aumentar las capacidades y potencialidades de la población en el marco de los principios y derechos que establece la Constitución. 5 Garantizar la soberanía nacional, promover la integración latinoamericana e impulsar una inserción estratégica en el contexto internacional, que contribuya a la paz y a un sistema democrático y equitativo mundial* ";

Que, el artículo 277 de la Constitución de la República determina que "*Para la consecución del buen vivir, serán deberes generales del Estado: 1 Garantizar los derechos de las personas, las colectividades y la naturaleza 2 Dirigir, planificar y regular el proceso de desarrollo 3 Generar y ejecutar las políticas públicas, y controlar y sancionar su incumplimiento 4 Producir bienes, crear y mantener infraestructura y proveer servicios públicos 5 Impulsar el desarrollo de las actividades económicas mediante un orden jurídico e instituciones políticas que las promuevan, fomenten y defiendan mediante el cumplimiento de la*

*Constitución y la ley 6 Promover e impulsar la ciencia, la tecnología, las artes, los saberes ancestrales y en general las actividades de la iniciativa creativa, comunitaria, asociativa, cooperativa y privada.*";

Que, el artículo 283 de la Carta Magna dispone que "*El sistema económico es social y solidario, reconoce al ser humano como sujeto y fin, propende a una relación dinámica y equilibrada entre sociedad, Estado y mercado, en armonía con la naturaleza, y tiene por objetivo garantizar la producción y reproducción de las condiciones materiales e inmateriales que posibiliten el buen vivir* ";

Que, el artículo 285 de la Norma Suprema prescribe que "*El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad 3 Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir* ";

Que, el numeral 1 del 387 de la Constitución de la República establece que "*Será responsabilidad del Estado 1 Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo* ";

Que, el artículo 416 de la Carta Maga preceptúa que "*Las relaciones del Ecuador con la comunidad internacional responderán a los intereses del pueblo ecuatoriano, al que le rendirán cuenta sus responsables y ejecutores, y en consecuencia 1 Proclama la independencia e igualdad jurídica de los Estados, la convivencia pacífica y la autodeterminación de los pueblos, así como la cooperación, la integración y la solidaridad 7 Exige el respeto de los derechos humanos, en particular de los derechos de las personas migrantes, y propicia su pleno ejercicio mediante el cumplimiento de las obligaciones asumidas con la suscripción de instrumentos internacionales de derechos humanos* ";

Que, el artículo 417 de la Norma Suprema dispone que "*Los tratados internacionales ratificados por el Ecuador se sujetarán a lo establecido en la Constitución En el caso de los tratados y otros instrumentos internacionales de derechos humano se aplicarán los principios pro ser humano, de no restricción de derechos, de aplicabilidad directa y de cláusula abierta establecidos en la Constitución* ",

Que, el numeral 3 del artículo 423 de la Constitución de la República prevé que "*La integración en especial con los países de Latinoamérica y el Caribe será un objetivo estratégico del Estado En todas las instancias y procesos de integración, el Estado ecuatoriano se comprometerá a 3 Fortalecer la armonización de las legislaciones nacionales con énfasis en los derechos (. ), de acuerdo con los principios de progresividad y no regresividad* ",

Que, el artículo 424 de la Carta Magna prescribe que "*La Constitución es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico Las normas y los actos del poder público deberán mantener conformidad con las disposiciones constitucionales, en caso contrario carecerán de eficacia jurídica. La Constitución y los tratados internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los contenidos en la Constitución, prevalecerán sobre cualquier otra norma jurídica o acto del poder público.*";

Que, el artículo 426 de la Norma Suprema establece que "*Todas las personas, autoridades e instituciones están sujetas a la Constitución ( ) Los derechos consagrados en la Constitución y los instrumentos internacionales de derechos humanos serán de inmediato cumplimiento y aplicación (. )* ";

Que, la Resolución 45/95 de 14 de diciembre de 1990 de la Organización de las Naciones Unidas adopta principios rectores para la reglamentación de los ficheros computarizados de datos personales, garantías mínimas que deberán preverse en legislaciones nacionales para efectivizar este derecho ;

Que, uno de los ejes de la Estrategia acordada en el año 2016 de la red Iberoamericana de Datos Personales 2020 consiste en "*Impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetros para futuras regulaciones o para revisión de las existentes en materia de protección de datos personales* ";

Que, el 20 de junio de 2017 se aprobaron los Estándares de Protección de Datos Personales para los Estados Iberoamericanos;

Que, el Comité Jurídico Interamericano de la Organización de Estados Americanos adoptó la propuesta de declaración de principios de privacidad y protección de datos personales en las Américas;

Que, la Organización de Estados Americanos el 27 de marzo de 2015 desarrolló el Proyecto de Ley Modelo sobre Protección de datos Personales;

Que, el Objetivo 1 del Eje 1: Derechos para todos durante toda la vida, del Plan Nacional de Desarrollo 2017-2021-Toda una Vida apunta a "*Garantizar una vida digna con iguales oportunidades para todas las personas* ";

Que, el Objetivo 5 del Eje 2. Economía al servicio de la sociedad, del plan Nacional de Desarrollo 2017-2021-Toda una Vida, persigue "*Impulsar la productividad y competitividad para el crecimiento económico y sostenible de manera redistributiva y solidaria.*",

Que, el Objetivo 7 del Eje 3: Más sociedad, mejor Estado; del plan Nacional de Desarrollo 2017-2021-Toda una Vida, busca "*Incentivar una sociedad participativa, con un Estado cercano al servicio de la ciudadanía.*";

Que, el Objetivo 8 del Eje 3 Más sociedad, mejor Estado; del plan Nacional de Desarrollo 2017-2021-Toda una Vida, pretende "*Promover la transparencia y la corresponsabilidad para una nueva ética social*",

Que, el Objetivo 9 del Eje 3: Más sociedad, mejor Estado; del plan Nacional de Desarrollo 2017-2021-Toda una Vida, aspira a "*Garantizar la soberanía y la paz, y posicionar estratégicamente al país en la región y el mundo* ";

Que, la protección de datos personales forma parte de los ejes estratégicos para la construcción de la sociedad de la información y el conocimiento en el Ecuador conforme el Libro Blanco de la Sociedad de la Información y del Conocimiento 2018;

Que, el Eje 6 del Plan de la Sociedad de la Información y del Conocimiento 2018-2021, busca "*Promover la protección de datos personales con enfoque de Gobierno, de empresa y para el ciudadano.*";

Que, la Acción Estratégica clave del enfoque para Gobierno de protección de datos personales del Eje 6 del Plan Nacional de la Sociedad de la Información y del Conocimiento 2018-2021, es "*Promulgar una ley orgánica de protección de datos personales para garantizar el derecho constitucional.*",

Que, el principio de Legalidad de la Carta Iberoamericana de Gobierno Electrónico del año 2007 establece que "*( ) el uso de comunicaciones electrónicas promovidas por la Administración Pública deberá tener observancia de las normas en materia de protección de datos personales*", con el objetivo de precautelar el derecho que tienen los ciudadanos a relacionarse electrónicamente con el Estado;

Que, la Estrategia Ecuador Digital, fomenta un Ecuador Eficiente y Ciberseguro, para lo cual, ha establecido que la Protección de Datos Personales es un eje esencial para alcanzarlo, en este sentido, determina como objetivo "*Concientizar a las decenas de miles de usuarios de los portales web del gobierno central acerca de cómo están siendo usados sus datos personales* ".

Que, la Estrategia Ecuador Digital, para alcanzar un Ecuador Eficiente y Ciberseguro, propone, como objetivo dentro del eje de Protección de Datos Personales, "*Poner freno al uso inapropiado de la información personal tanto en el ámbito público como privado.*".

Que, la Estrategia 3 del Programa de Gobierno Abierto del Plan Nacional de Gobierno Electrónico apunta a "*Impulsar la protección de la información y datos personales* "; y,

En uso de la atribución que le confiere el número 6 del artículo 120 de la Constitución de la República, expide la siguiente:

## LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES

### CAPÍTULO I
### DISPOSICIONES DIRECTIVAS

***Artículo 1. Objeto***: El objeto de la presente Ley es regular el ejercicio del derecho a la protección de datos personales, la autodeterminación informativa y demás derechos digitales en el tratamiento y flujo de datos personales, a través del desarrollo de principios, derechos, obligaciones y mecanismos de tutela.

***Artículo 2. Finalidad***: La finalidad de la presente Ley es procurar el adecuado tratamiento y flujo de datos personales para garantizar los derechos fundamentales y las libertades individuales, promover el progreso económico y social; impulsar la producción nacional y la cooperación internacional; fomentar la competitividad, la innovación y productividad, elevar la eficiencia de los servicios públicos y/o privados; y, mejorar la calidad de vida.

***Artículo 3. Ámbito de aplicación material***: La presente Ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, ya sean totalmente automatizados, parcialmente automatizados o no automatizados y a toda modalidad de uso posterior, por parte de responsables o encargados del tratamiento de datos personales.

La presente ley no será aplicable a:

1. El tratamiento de datos personales utilizados en actividades familiares o domésticas;
2 Datos anónimos, y,
3 Datos que identifican o hacen identificable a personas jurídicas

Son accesibles al público y susceptibles de tratamiento los datos personales de contacto de comerciantes; representantes y socios de personas jurídicas; así como los de servidores públicos siempre y cuando se refieran al ejercicio de su profesión, oficio, giro de negocio, competencias, facultades, atribuciones o cargo.

El histórico y vigente de la declaración patrimonial y de la remuneración para el caso de servidores públicos, por la naturaleza de su cargo, se considerará accesible al público y susceptible de tratamiento.

***Artículo 4. Ámbito de aplicación territorial***: Sin perjuicio de la normativa establecida en los instrumentos internacionales ratificados por el Estado ecuatoriano que versen sobre esta materia se aplicará la presente Ley cuando:

1. El tratamiento de datos personales se realice en cualquier parte del territorio nacional;
2. El responsable o encargado del tratamiento de datos personales se encuentre domiciliado en cualquier parte del territorio nacional;
3. El responsable o encargado del tratamiento de datos personales que no se encuentre domiciliado en el Ecuador y oferte bienes o servicios a personas localizadas en el territorio nacional, independientemente de si se requiere su pago o no,
4. El responsable o encargado del tratamiento de datos personales que no se encuentre domiciliado en el Ecuador y realice actividades relativas a la recogida de datos personales de personas localizadas en el territorio nacional; y,
5. Al responsable o encargado del tratamiento de datos personales no domiciliado en el territorio nacional que le resulte aplicable la legislación nacional, en virtud de la celebración de un contrato o del derecho internacional público.

***Artículo 5. Términos y definiciones***: Para los efectos de la aplicación de la presente Ley se establecen las siguientes definiciones:

***Anonimización:*** La aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o re-identificación de una persona natural sin esfuerzos desproporcionados.

***Base de datos:*** Conjunto configurado, estructurado o no estructurado de datos, cualquiera que fuere la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, tratamiento, procesamiento y acceso.

***Consentimiento:*** Manifestación de voluntad libre, previa, específica, expresa, informada e inequívoca, por la que el titular de los datos personales autoriza al responsable del tratamiento de datos personales a tratar los mismos.

***Dato biométrico:*** Dato personal único obtenido a partir de un tratamiento técnico-específico, relativo a las características físicas, fisiológicas o conductuales de una persona natural que permita o confirme la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos, entre otros

***Dato genético:*** Dato personal único relacionado a características genéticas heredadas o adquiridas de una persona natural que proporcionan información única sobre la fisiología o salud de un individuo; generalmente se analizan a partir de muestras biológicas.

***Dato personal:*** Dato que identifica o hace identificable a una persona natural, directa o indirectamente, en el presente o futuro. Los datos inocuos, metadatos o fragmentos de datos que identifiquen o hagan identificable a un ser humano, forman parte de este concepto.

***Datos personales crediticios:*** Datos que integran el comportamiento de personas naturales para analizar su capacidad de pago y financiera.

***Datos personales registrables:*** Datos personales que conforme al ordenamiento jurídico deben estar contenidos en Registros Públicos

***Datos sensibles:*** Se consideran datos sensibles los relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos humanos o la dignidad e integridad de las personas. La Autoridad de Protección de Datos Personales podrá determinar otras categorías de datos sensibles

***Destinatario:*** Persona natural o jurídica que ha recibido comunicación de datos personales.

***Disociación de datos:*** Todo tratamiento de datos personales destinado a que éstos no puedan ser asociados o vinculados a una persona identificada o identificable.

***Elaboración de perfiles:*** Todo tratamiento de datos personales que permite evaluar, analizar o predecir aspectos de una persona natural para determinar comportamientos o patrones relativos a: rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, ubicación, movimiento físico de una persona, entre otros.

***Encargado del tratamiento de datos personales:*** Persona que trate datos personales por nombre y a cuenta de un responsable de tratamiento de datos personales.

***Estado de la técnica:*** Estado último de cualquier particularidad que permita establecer bases de comparación para determinar si los requisitos o herramientas de carácter administrativo, físico, técnico, organizativo, jurídico u otros constituyen niveles adecuados de protección en el tratamiento de datos personales.

***Filtración:*** Es un incidente ilegal o no autorizado que involucra la visualización, acceso, extracción o divulgación de datos personales por un individuo, aplicación, servicio u otros.

***Fuentes accesibles al público:*** Bases de datos que pueden ser consultadas por cualquier persona natural o jurídica, pública o privada, nacional o internacional cuyo acceso no se encuentre limitado por la normativa vigente o disposición de la Autoridad de Protección de Datos Personales

***Política de tratamiento de datos personales:*** Documento físico, electrónico o en cualquier formato generado por el responsable del tratamiento de datos personales que debe obligatoriamente ponerse a

disposición del titular, a partir del momento en el cual se recaben sus datos personales y debe estar disponible de forma permanente, con el objeto de garantizar el derecho a la transparencia, cuyo contenido será definido por la Autoridad de Protección de Datos Personales.

***Responsable del tratamiento de datos personales:*** Persona natural o jurídica, pública o privada, que decide sobre la finalidad y el tratamiento de datos personales

***Sellos de Protección de Datos Personales:*** Acreditación que otorga la Entidad Certificadora al responsable o al encargado del tratamiento de datos personales, de haber implementado mejores prácticas en sus procesos, con el objetivo de promover la confianza del titular, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

***Tercero:*** Persona que no ostenta la calidad de responsable o encargado de tratamiento; titular; o, Autoridad de Protección de Datos Personales, conforme al alcance establecido en la presente Ley.

***Titular:*** Persona natural cuyos datos son objeto de tratamiento.

***Transferencia o comunicación:*** Manifestación, declaración, publicación, entrega, consulta, interconexión, cesión, transmisión, difusión, divulgación o cualquier forma de revelación de datos personales realizada a una persona distinta al titular, responsable o encargado del tratamiento de datos personales. Los datos personales que han de comunicarse deben ser exactos, completos y actualizados.

***Tratamiento:*** Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, comunicación por transmisión, transferencia, difusión, procesamiento, almacenamiento, distribución, cesión, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales.

***Vulneración de la seguridad de los datos personales:*** Incidente de seguridad que afecta la confidencialidad, disponibilidad o integridad de los datos personales, como por ejemplo la filtración.

***Artículo 6. Sujetos intervinientes:*** Son parte del sistema de protección de datos personales, lo siguientes sujetos:

1. Titular,
2. Responsable del tratamiento;
3. Encargado del tratamiento;
4. Tercero;
5 Destinatario;
6. Autoridad de protección de datos;
7. Entidades certificadoras; y,
8. Delegado de protección de datos personales.

***Artículo 7. Normas aplicables al ejercicio de derechos:*** El ejercicio de los derechos a la protección de datos personales, se canalizará a través del responsable del tratamiento, Autoridad de Protección de Datos Personales y/o jueces competentes, de conformidad con el procedimiento establecido en la presente ley.

## CAPÍTULO II
## PRINCIPIOS

***Artículo 8. Principios***: Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de juridicidad, lealtad y transparencia, legitimidad, finalidad; pertinencia y minimización de datos personales; proporcionalidad del tratamiento: consentimiento; confidencialidad, calidad, conservación; seguridad de datos personales; responsabilidad proactiva y demostrada, aplicación favorable al titular; e, independencia de control.

***Artículo 9. Juridicidad, lealtad y transparencia***: Los datos personales deben tratarse con estricto apego y cumplimiento a los principios, derechos y obligaciones establecidas en la Constitución, los instrumentos internacionales, la presente Ley, su reglamento y la demás normativa y jurisprudencia aplicable.

En ningún caso los datos personales podrán ser tratados a través de medios o para fines ilícitos o desleales.

Las relaciones derivadas del tratamiento de datos personales deben ser transparentes y se rigen en función de las disposiciones contenidas en la presente Ley, su reglamento y demás normativa atinente a la materia.

***Artículo 10. Legitimidad:*** El tratamiento solo será legítimo y lícito si se cumple con alguna de las siguientes condiciones:

1. Exista obligación en el ordenamiento jurídico aplicable al responsable del tratamiento;
2. Por orden judicial, resolución o mandato motivado de autoridad pública competente;
3. Para el ejercicio de las competencias y facultades establecidas en la Constitución, la Ley, instrumentos internacionales ratificados por el Ecuador y demás normativa aplicable a favor de las entidades pertenecientes al sector público, sus delegatarios y organizaciones de Derecho Internacional Público;
4. Para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado,
5. Para la ejecución de medidas precontractuales a petición del titular, excepto cuando prevalezcan los intereses o los derechos y libertades de niñas, niños y adolescentes como titulares;
6. Por consentimiento del titular para el tratamiento de sus datos personales para una o varias finalidades específicas; o,
7. Para proteger intereses vitales, del interesado o de otra persona natural, como por ejemplo su vida, salud o integridad.

***Artículo 11. Finalidad***: Las finalidades del tratamiento deberán ser determinadas, explícitas y legítimas, no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme el principio de legitimidad.

***Artículo 12. Pertinencia y Minimización de datos personales***: Los datos personales deben ser pertinentes y limitados a lo mínimo necesario para su finalidad

***Artículo 13. Proporcionalidad del tratamiento:*** El tratamiento debe ser adecuado, necesario, oportuno, relevante y no excesivo en relación a las finalidades para las cuales han sido recogidos o a la naturaleza de las categorías especiales de datos.

***Artículo 14. Consentimiento***: Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular de hacerlo.

El consentimiento será válido, cuando la manifestación de la voluntad sea: *libre*, es decir, que se encuentre exenta de vicios del consentimiento, *especificidad*, se refiere a la determinación concreta de los medios y fines del tratamiento, *informada*, aquella que cumple con el principio de transparencia y efectiviza el derecho a la transparencia; *inequívoca*, que no se presenten dudas sobre el alcance de la autorización otorgada por el titular; *previa*, que el consentimiento se haya dado con anterioridad al tratamiento, ya sea en el momento mismo de la recogida del dato cuando se obtiene directamente del titular y excepcionalmente de forma posterior cuando los datos personales no se obtuvieren de forma directa; *expresa*, que de manera indubitable el responsable pueda demostrar que el titular manifestó su voluntad a través de una declaración o acción clara, afirmativa o se deduzca de una acción del titular.

El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento igual de sencillo que el que fue llevado para recabar el consentimiento.

El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos.

***Artículo 15. Confidencialidad***. El tratamiento de datos personales debe concebirse sobre la base del debido sigilo y secreto, es decir, no deben tratarse o comunicarse para un fin distinto para el cual fueron recogidos, sin que se cuente con el consentimiento del titular o concurra una de las causales que habiliten el tratamiento conforme al principio de legitimidad. El nivel de confidencialidad dependerá de la naturaleza del dato personal

Este principio no implica solamente el mantenimiento de la seguridad de los datos personales, sino también la facultad del titular de controlar la forma en la que se tratan sus datos, incluyendo la transferencia o comunicación

***Artículo 16. Calidad*** Los datos personales que sean objeto de tratamiento deben ser exactos, íntegros; precisos; completos, comprobables; claros; y, de ser el caso, debidamente actualizados; de tal forma que no se altere su veracidad

La Autoridad de Protección de Datos Personales definirá los casos en los cuales se deberán actualizar los datos personales y su periodicidad

***Artículo 17. Conservación***. Los datos personales serán conservados conforme a los siguientes presupuestos:

1. Durante el tiempo consentido, determinado en el ordenamiento jurídico o establecido en orden judicial, resolución o mandato motivado de autoridad pública competente; o,

2. Hasta cuando cumplan con la finalidad para la cual fueron recogidos o tratados.

Cumplido uno de los presupuestos establecidos, los datos personales deberán suprimirse o ser sometidos a un proceso de anonimización, de ser el caso. Para lo cual, el responsable implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura los datos personales.

El posterior tratamiento de datos personales únicamente se realizará para la investigación científica, histórica o estadística, que se realice en favor del interés público, siempre y cuando se establezcan las garantías de seguridad y protección de datos personales oportunas, así como las demás que contemple la presente Ley, su Reglamento de Aplicación o las Resoluciones de la Autoridad de Protección de Datos Personales, para salvaguardar los derechos contemplados en esta norma.

***Artículo 18. Seguridad de datos personales***: Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, sean éstas técnicas, organizativas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.

***Artículo 19. Responsabilidad proactiva y demostrada***: El responsable del tratamiento de datos personales deberá acreditar el haber implementado mecanismos para la protección de datos personales; es decir, el cumplimiento de los principios, derechos y obligaciones establecidos en la presente Ley, para lo cual, además de lo establecido en la normativa aplicable, podrá valerse de estándares, mejores prácticas, esquemas de auto y corregulación, códigos de protección, sistemas de certificación, sellos de protección de datos personales o cualquier otro mecanismo que se determine adecuado a los fines, la naturaleza del dato personal o el riesgo del tratamiento.

El responsable del tratamiento de datos personales está obligado a rendir cuentas sobre el tratamiento al titular y a la Autoridad de Protección de Datos Personales

El responsable del tratamiento de datos personales deberá evaluar y revisar los mecanismos que adopte para cumplir con el principio de responsabilidad de forma continua y permanente, con el objeto de mejorar su nivel de eficacia en cuanto a la aplicación de la presente Ley.

***Artículo 20. Aplicación favorable al titular***: En caso de duda sobre el alcance de las disposiciones del ordenamiento jurídico o contractuales, aplicables a la protección de datos personales, los funcionarios judiciales y administrativos las interpretarán y aplicarán en el sentido más favorable al titular de dichos datos.

***Artículo 21. Independencia de control***: Para el efectivo ejercicio del derecho a la protección de datos personales, el Estado ejercerá un control independiente, imparcial y autónomo, así como su regulación y sanción.

***Artículo 22. Normativa especializada:*** Los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias

atribuidas en la normativa vigente, estarán sujetos a los principios establecidos en sus propias normas y los principios de juridicidad, lealtad y transparencia; legitimidad; finalidad; confidencialidad; conservación, seguridad de datos personales, responsabilidad proactiva y demostrada, en los casos que corresponda, y, de aplicación favorable.

## CAPÍTULO III
## DERECHOS

***Artículo 23. Derecho a la lealtad, transparencia e información*** · El titular de datos personales tiene derecho a ser informado de forma leal y transparente por cualquier medio sobre.

1. Los fines del tratamiento;
2. Base legal para el tratamiento;
3 Tipos de tratamiento;
4 Tiempo de conservación;
5. La existencia de una base de datos en donde consten sus datos personales;
6. El origen de los datos personales cuando no se hayan obtenido directamente del titular;
7 Otras finalidades y tratamientos ulteriores;
8. Identidad y datos de contacto del responsable del tratamiento de datos personales, que incluye: dirección de domicilio legal, número de teléfono y correo electrónico,
9. Identidad y datos de contacto del delegado de protección de datos personales, que incluye: dirección domiciliaria, teléfono y correo electrónico;
10. Las transferencias o comunicaciones, nacionales o internacionales, de datos personales que pretenda realizar, incluyendo los destinatarios y sus clases, así como las finalidades que motivan la realización de estas;
11. Carácter obligatorio o facultativo de la respuesta y las consecuencias de proporcionar o no sus datos personales;
12. El efecto de suministrar datos personales erróneos o inexactos;
13. La posibilidad de revocar el consentimiento;
14. La existencia y forma en que pueden hacerse efectivos sus derechos de acceso, eliminación, rectificación y actualización, oposición, anulación, limitación del tratamiento y a no ser objeto de una decisión basada únicamente en valoraciones automatizadas;
15. Los mecanismos para hacer efectivo su derecho a la portabilidad, cuando el titular lo solicite;
16. Dónde y cómo realizar sus reclamos ante el responsable del tratamiento de datos personales, y la Autoridad de Protección de Datos Personales, y,
17. La existencia de valoraciones y decisiones automatizadas, incluida la elaboración de perfiles.

En el caso que los datos fueran obtenidos directamente del titular, la información deberá ser comunicada de forma previa a este, es decir, en el momento mismo de la recogida del dato personal.

Excepcionalmente, el titular deberá ser informado de forma posterior, dentro del mes siguiente, cuando los datos personales no se obtuvieren de forma directa, expresa; transparente; inteligible, concisa; precisa; sin barreras técnicas; e, inequívoca

Con el objeto de que pueda autorizar el tratamiento, transferencia o comunicación de sus datos personales, esta información deberá ser proporcionada al titular de forma accesible por cualquier medio, incluidas

políticas de protección de datos personales, gratuitos; suficientes; disponibles de forma permanente y redactarse en un lenguaje claro, sencillo; y, de fácil comprensión incluso cuando se trate de contratación electrónica.

En el caso de productos o servicios dirigidos, utilizados o que pudieran ser utilizados por niñas, niños y adolescentes, la información a la que hace referencia el presente artículo será proporcionada a su representante legal conforme a lo dispuesto en el inciso precedente.

***Artículo 24. Derecho de Acceso***: El titular tiene derecho a conocer y a obtener del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna.

El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el ejercicio de este derecho.

En caso de que fuera necesario restringir o negar dicho acceso, deberán especificarse las razones concretas de dicha restricción o negativa de acuerdo a lo establecido en la normativa vigente.

***Artículo 25. Derecho de Rectificación y Actualización***: El titular tiene el derecho de solicitar se corrijan o actualicen sus datos inexactos, incompletos, desactualizados, erróneos, falsos, incorrectos o imprecisos

***Artículo 26. Derecho de Eliminación***: El titular tiene derecho a solicitar la supresión de sus datos personales, a fin de que estos dejen de ser tratados por el responsable del tratamiento de datos personales, cuando:

1. El tratamiento no cumpla con los principios de juridicidad, lealtad, transparencia y legitimidad;
2. El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;
3. Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;
4 Haya vencido el plazo de conservación de los datos personales;
5. El tratamiento afecte derechos fundamentales o libertades individuales; o
6. Haya revocado o no haya otorgado el consentimiento para uno o varios fines específicos, sin necesidad de que medie justificación alguna.

El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales

***Artículo 27. Derecho al olvido digital***· El titular tiene el derecho a solicitar al juez competente, obtener sin dilación indebida del responsable del tratamiento la supresión de sus datos personales que estén siendo tratados en el entorno digital, cuando concurra alguna de las circunstancias siguientes:

1. Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados;
2. El interesado retire el consentimiento en que se basa el tratamiento o solicite su supresión,
3. El interesado se oponga al tratamiento, y no prevalezcan otros motivos legítimos para el tratamiento;
4 Los datos personales hayan sido tratados ilícitamente,
5 Los datos personales sean de carácter obsoleto;

6. Los datos personales no tengan valor histórico o científico;
7. Los datos personales no sean de relevancia pública; o,
8 Los datos personales sean inadecuados, inexactos, impertinentes o excesivos con relación a los fines y al tiempo transcurrido

Lo anterior no se aplicará cuando el tratamiento sea necesario por cualquiera de las siguientes causas.

1 Para ejercer el derecho a la libertad de expresión e información;
2 Para el cumplimiento de una obligación legal que requiera el tratamiento de datos por parte del responsable del tratamiento,
3. Por razones de interés público en el ámbito de la salud pública;
4. Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos; o,
5. Para la formulación, el ejercicio o la defensa de reclamaciones

Para la aplicación del presente artículo, se estará a las siguientes definiciones:

***Datos personales tratados en el entorno digital:*** Datos personales que son tratados en redes de computadoras públicas o privadas (Internet o Intranet). Se entiende por redes privadas aquellas que no están abiertas al acceso de todo público pero que si son usadas por una colectividad de usuarios autorizados.

***Datos personales de carácter obsoleto:*** Datos personales que ya no están en uso, son antiguos, anticuados o han dejado de tener vigencia o relevancia para los fines del tratamiento.

***Datos personales que no tengan valor histórico o científico:*** Datos personales que no son útiles, necesarios o de valor significativo para la ciencia o la historia política o social de Ecuador.

***Datos personales que no sean de relevancia pública:*** Datos personales que el público en general no necesita o no tiene interés justificado en conocer.

***Artículo 28. Derecho de oposición:*** El titular tiene el derecho a oponerse o negarse al tratamiento de sus datos personales, en especial para fines de mercadotecnia, valoraciones o decisiones automatizas incluida la elaboración de perfiles.

***Artículo 29. Derecho de anulación:*** El titular tiene derecho a solicitar la nulidad por ilicitud en el acto o por el tratamiento de datos personales ante autoridad jurisdiccional, bajo las causales señaladas para la nulidad en materia civil, mercantil y administrativa, según sea el caso.

***Artículo 30. Derecho a la portabilidad:*** El titular tiene derecho a recibir del responsable del tratamiento, sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; y/o transmitirlos a otros responsables.

El titular podrá solicitar la transferencia o comunicación de sus datos personales a otro responsable del tratamiento. Luego de completada la transferencia, el responsable que transfiere dichos datos procederá a su eliminación.

Para que proceda el derecho a la portabilidad de datos es necesario que se produzca al menos una de las siguientes condiciones:

1. Que el titular haya otorgado su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos, la transferencia o comunicación se hará entre responsables del tratamiento de datos personales cuando la operación sea técnicamente posible;
2. Que el tratamiento se efectúe por medios automatizados;
3. Que se trate de un volumen relevante de datos personales; o,
4. Que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos del responsable o encargado del tratamiento de datos personales, o del titular en el ámbito del derecho laboral y seguridad social.

Esta transferencia o comunicación debe ser económica y financieramente eficiente, expedita, efectiva y sin trabas.

No procederá este Derecho cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable del tratamiento de datos personales con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

***Artículo 31. Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad:*** No proceden los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad, en los siguientes casos:

1. Si el solicitante no es el titular de los datos personales o su representante legal no se encuentre debidamente acreditado;
2 Para el cumplimiento de una obligación legal o contractual;
3. Para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente,
4. Para la formulación, ejercicio o defensa de reclamos o recursos,
5. Cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros;
6. Cuando se pueda obstaculizar actuaciones judiciales o administrativas en curso debidamente notificadas;
7. Para ejercer el derecho a la libertad de expresión y opinión;
8 Para proteger el interés vital del interesado o de otra persona natural;
9 En los casos en que medie el interés público; o,
10. En el tratamiento de datos personales que sean necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística

***Artículo 32. Derecho a la limitación del tratamiento:*** El titular tendrá derecho a que se use el mínimo de sus datos personales en el tratamiento efectuado por responsables o encargados del tratamiento de datos personales, a que sus datos personales no se encuentren disponibles en internet u otros medios de comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido a los titulares o a los autorizados por razones de interés público; a que el tratamiento de datos personales se limite al período que medie entre una solicitud de revisión de juridicidad, lealtad, transparencia, legitimidad, acceso, eliminación, rectificación y actualización, oposición, anulación, portabilidad, limitación del tratamiento o, de no ser objeto de una decisión basada únicamente en

valoraciones automatizadas, hasta su resolución por el responsable o encargado del tratamiento de datos personales.

De existir negativa por parte del responsable o encargado del tratamiento de datos personales, y el titular recurra por dicha decisión ante la Autoridad de Protección de Datos Personales, esta limitación se extenderá hasta la resolución del procedimiento administrativo.

El responsable del tratamiento de datos personales conservará únicamente los datos personales que sean necesarios para la formulación de un reclamo, una vez cumplido el plazo o condición del tratamiento.

***Artículo 33. Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas:*** El titular tiene derecho a no ser sometido a una decisión basada únicamente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales, para lo cual podrá:

1. Solicitar una explicación motivada sobre la decisión tomada por el responsable o encargado del tratamiento de datos personales;
2 Presentar observaciones;
3 Solicitar los criterios de valoración sobre el programa automatizado; y/o,
4. Impugnar la decisión ante el responsable o encargado de tratamiento

No se aplicará este derecho cuando:

1 La decisión es necesaria para la celebración o ejecución de un contrato entre el titular y el responsable o encargado del tratamiento de datos personales;
2 Está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad pública competente, para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular; o,
3. Se base en el consentimiento del titular.

***Artículo 34. Derecho de consulta***: Las personas tienen derecho a la consulta pública y gratuita ante el Registro Nacional de Protección de Datos Personales, de conformidad con la presente ley

***Artículo 35. Derecho a la educación digital***: Las personas tienen derecho al acceso y disponibilidad del conocimiento, aprendizaje, preparación, estudio, formación, capacitación, enseñanza e instrucción relacionados al uso y manejo adecuado, sano, constructivo, seguro y responsable de las tecnologías de la información y comunicación, en estricto apego a la dignidad e integridad humana, los derechos fundamentales y libertades individuales con especial énfasis en la intimidad, la vida privada, autodeterminación informativa, identidad y reputación en línea, ciudadanía digital y el derecho a la protección de datos personales

El órgano rector de la educación, en coordinación con la Autoridad de Protección de Datos, emitirá las directrices para que las entidades educativas garanticen el enfoque de derechos antes mencionados de manera transversal en el currículo nacional en todos los niveles educativos. Se deberán emprender proyectos orientados a la prevención de situaciones de riesgo derivadas de la inadecuada utilización de las tecnologías de la información y comunicación, con especial atención a las situaciones de violencia en la red.

El cuerpo docente deberá ser formado y capacitado en competencias digitales para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior

Los planes de estudio de los títulos universitarios, en especial aquellos que habiliten el desempeño profesional relacionado con la formación de niñas, niños y adolescentes, garantizarán el conocimiento en el uso y seguridad de los medios digitales y en el efectivo ejercicio de los derechos fundamentales en Internet.

***Artículo 36. Ejercicio de derechos***: El Estado, entidades educativas, organizaciones de la sociedad civil, proveedores de servicios de la sociedad de la información y el conocimiento, y otros entes relacionados, dentro del ámbito de sus relaciones, están obligados a proveer información y capacitación relacionada al uso y tratamiento responsable, adecuado y seguro de datos personales de niñas, niños y adolescentes, tanto a sus titulares como a sus representantes legales, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

Los adolescentes mayores a doce (12) años y menores de dieciséis (16) años, así como las niñas y niños, para el ejercicio de sus derechos necesitarán de su representante legal Los adolescentes mayores a dieciséis (16) años y menores de dieciocho (18) años, podrán ejercitarlos de forma directa ante la Autoridad de Protección de Datos Personales o ante el responsable de la base de datos personales y del tratamiento.

Los derechos del titular son irrenunciables. Será nula toda estipulación en contrario.

***Artículo 37. Excepción por normativa especializada:*** No proceden los derechos establecidos en esta ley, para los datos personales cuyo tratamiento se encuentre regulado en normativa especializada en materia de ejercicio de la libertad de expresión, gestión de riesgos, desastres naturales, seguridad nacional y defensa del Estado; y, los datos personales que deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente En estos casos, los titulares podrán ejercer los derechos previstos en dicha normativa especializada.

## CAPÍTULO IV
## CATEGORÍAS ESPECIALES DE DATOS PERSONALES

***Artículo 38. Categorías especiales de datos personales***: Se aplicará lo dispuesto en el presente capítulo al tratamiento de datos sensibles, datos de niñas, niños y adolescentes, datos crediticios, datos de salud y datos necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.

***Artículo 39. Consentimiento relativo a categorías especiales de datos***: Además de los requisitos del consentimiento previstos en el artículo 13, se requiere de la manifestación de la voluntad explícita del titular para el tratamiento de datos sensibles, datos crediticios y de datos personales de adolescentes mayores a dieciséis (16) años y menores de dieciocho (18) años.

Para el caso de adolescentes mayores a doce (12) años y menores de dieciséis (16) años, así como de niñas y niños, es necesario contar con el consentimiento explícito y verificable de su representante legal. La Autoridad de Protección de Datos Personales definirá los parámetros de verificación del consentimiento.

Se entiende por consentimiento explícito aquel que puede ser demostrado de manera indubitable por el responsable o encargado del tratamiento de datos personales, en relación a la autorización otorgada por el titular a través de una declaración o acción clara y afirmativa.

El responsable o encargado del tratamiento de datos personales está en obligación de verificar si el titular o representante legal ha otorgado su consentimiento explícito para el tratamiento de datos sensibles, datos crediticios y en especial, datos de niñas, niños y adolescentes.

***Artículo 40. Lealtad, transparencia e información de categorías especiales de datos:*** Además de la información establecida en el derecho a la lealtad, transparencia e información, el responsable o encargado del tratamiento de datos personales, deberá informar al titular o al representante legal, del carácter facultativo de sus respuestas, consecuencias y los derechos que le asisten al titular, respecto de datos sensibles y de datos de niñas, niños y adolescentes

***Artículo 41. Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas en categorías especiales de datos:*** Además de los presupuestos establecidos en el derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas, no se podrán tratar datos sensibles o datos de niñas, niños y adolescentes, a menos que se cuente con autorización explícita del titular o representante legal; o, cuando dicho tratamiento esté destinado a salvaguardar el interés público.

***Artículo 42. Datos de personas fallecidas***: Los titulares de derechos sucesorios del fallecido, podrán dirigirse al responsable del tratamiento de datos personales con el objeto de solicitar el acceso, rectificación y actualización o eliminación de los datos personales del causante

Las personas o instituciones que el fallecido haya designado expresamente para ello, podrán también solicitar con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste; y, en su caso su rectificación, actualización o eliminación.

En caso de fallecimiento de niñas, niños, adolescentes o personas a las que la Ley reconoce como incapaces, las facultades de acceso, rectificación y actualización o eliminación, podrán ejercerse por quién hubiese sido su último representante legal.

El ejercicio de este derecho estará regulado en el Reglamento a la presente Ley.

***Artículo 43. Tratamiento de datos personales necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística***: Para el tratamiento de datos personales necesarios para el archivo de información que constituya patrimonio del Estado catalogados como tal por la ley de la materia, la investigación científica; histórica; o, estadística se sujetará a lo previsto a la normativa aplicable, y subsidiariamente a lo dispuesto en la presente Ley, su Reglamento y demás normativa dictada por la Autoridad de Protección de Datos Personales.

***Artículo 44. Datos crediticios***: La protección de datos personales crediticios se sujetará a lo previsto en la presente ley, en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales.

***Artículo 45. Datos relativos a la salud***: Las instituciones y centros sanitarios públicos y privados, así como los profesionales correspondientes, podrán tratar datos personales relativos a la salud de sus pacientes, de

acuerdo a lo previsto en la presente ley, en la legislación especializada sobre la materia y demás normativa dictada por la Autoridad de Protección de Datos Personales.

## CAPÍTULO V
## TRANSFERENCIA O COMUNICACIÓN Y ACCESO A DATOS PERSONALES POR TERCEROS

***Artículo 46. Transferencia o comunicación de datos personales.*** Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario y, además, se cuente con el consentimiento del titular.

***Artículo 47. Acceso a datos personales por parte de terceros.*** El acceso de un tercero a datos personales, no se considerará transferencia o comunicación, siempre que sea necesario para la prestación de un servicio al responsable del tratamiento de datos personales. El tercero que ha accedido legítimamente a datos personales en estas condiciones, será considerado encargado de tratamiento.

El tratamiento de datos personales realizado por terceros deberá estar regulado por un contrato, en donde se establezca de manera clara y precisa que el encargado del tratamiento de datos personales únicamente tratará los mismos conforme las instrucciones del responsable y que no los aplicará o utilizará para finalidades diferentes a las que figuren en el contrato, ni que los transferirá o comunicará, ni siquiera para su conservación, a otras personas.

Una vez que se haya cumplido la prestación contractual, los datos personales deberán ser destruidos o devueltos al responsable del tratamiento de datos personales.

El tercero será responsable de las infracciones derivadas de incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.

***Artículo 48. Excepciones de consentimiento para la transferencia o comunicación de datos personales:*** No es necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales, en los siguientes supuestos.

1. Cuando los datos han sido recogidos de fuentes accesibles al público;
2. Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica entre el responsable de tratamiento y el titular, cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con bases de datos;

   En este caso la transferencia o comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique,
3. Cuando los datos personales deban proporcionarse a autoridades administrativas o judiciales en virtud de solicitudes y órdenes amparadas en competencias atribuidas en la normativa vigente;
4 Cuando la comunicación se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos, siempre y cuando dichos datos se encuentren debidamente disociados, y,
5. Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre salud.

Cuando, sea requerido el consentimiento del titular para que sus datos personales sean comunicados a un tercero, éste puede revocarlo en cualquier momento, sin necesidad de que medie justificación alguna

La presente ley obligatoriamente debe ser aplicada por el destinatario, por el solo hecho de la comunicación de los datos; a menos que estos hayan sido anonimizados o sometidos a un proceso de disociación.

***Artículo 49. Falta de consentimiento para la transferencia o comunicación de datos personales.*** Se entenderá que no hubo consentimiento para la transferencia o comunicación de datos personales cuando el responsable del tratamiento no haya entregado información suficiente al titular, que le permita conocer la finalidad a que se destinarán sus datos o el tipo de actividad del tercero a quien se pretende transferir o comunicar dichos datos.

## CAPÍTULO VI
## SEGURIDAD DE DATOS PERSONALES

***Artículo 50. Seguridad de datos personales:*** El responsable o encargado del tratamiento de datos personales, según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos y el nivel de impacto que estos representen a los derechos fundamentales y libertades individuales.

El responsable o encargado del tratamiento de datos personales, deberá implementar un proceso de verificación, evaluación y valoración continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole implementadas con el objeto de garantizar y mejorar la seguridad del tratamiento de datos personales.

El responsable o encargado del tratamiento de datos personales deberá demostrar que las medidas adoptadas e implementadas mitiguen de forma adecuada los riesgos identificados.

Entre otras medidas, se podrán incluir las siguientes:

1. Medidas de anonimización, encriptación, cifrado o codificación de datos personales;
2. Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios del tratamiento de datos personales y el acceso a los datos personales, de forma rápida en caso de incidentes; y,
3 Medidas dirigidas a mejorar la resiliencia técnica, física, administrativa, organizativa, y jurídica.

Los responsables y encargados del tratamiento de datos personales, podrán acogerse a estándares para medición y gestión de riesgos, así como para la implementación y manejo de sistemas de seguridad de la información o a códigos de conducta reconocidos y autorizados por la Autoridad de Protección de Datos Personales.

***Artículo 51. Medidas de seguridad en el ámbito del sector público:*** El mecanismo gubernamental de seguridad de la información incluirá las medidas que deban implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados,

pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales.

El alcance de aplicación del mecanismo gubernamental de seguridad de la información, que incluya las disposiciones establecidas en el primer párrafo del presente artículo, abarcará a todos los miembros del sector público, conforme a lo detallado en el artículo 225 de la Constitución de la República del Ecuador.

Las instituciones mencionadas en el párrafo precedente podrán incorporar medidas adicionales a las establecidas en el mecanismo gubernamental de seguridad de la información, atendiendo a la naturaleza de sus atribuciones y funciones.

***Artículo 52. Protección de datos personales desde el diseño y por defecto***: El responsable y el encargado implementarán las medidas técnicas, organizativas y de cualquier otra índole con miras a garantizar que los procesos y medios de tratamiento protejan los datos personales desde su diseño, así como sus configuraciones se encuentren por defecto en cumplimiento de las disposiciones de la presente Ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia

***Artículo 53. Análisis de riesgo y determinación de medidas de seguridad aplicables***: Para el análisis de riesgos, amenazas y vulnerabilidades, el responsable y el encargado del tratamiento de datos personales deberán utilizar una metodología que considere, entre otros·

1. Las particularidades del tratamiento;
2. Las particularidades de las partes involucradas, y,
3 El tipo y volumen de datos personales objeto del tratamiento.

Para determinar las medidas de seguridad necesarias y adecuadas, se deberán tomar en cuenta, entre otros

1. Los resultados del análisis de riesgos, amenazas y vulnerabilidades;
2. La naturaleza de los datos personales;
3. Las características de las partes involucradas; y,
4. Los antecedentes de destrucción de datos personales, pérdida, alteración, divulgación o impedimento de acceso al titular a los mismos, sean éstas accidentales o intencionales, por acción u omisión, así como los de transferencia, comunicación, o acceso no autorizados o en exceso de autorización a dichos datos.

El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conlleven un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.

***Artículo 54. Evaluación de impacto del tratamiento de datos personales***: El responsable realizará una evaluación de impacto del tratamiento de datos personales cuando se ha identificado la probabilidad de que dicho tratamiento, por su naturaleza, contexto o fines, conlleva un alto riesgo para los derechos y libertades del titular.

La evaluación de impacto del tratamiento de datos personales podrá analizar un conjunto de tratamientos equivalentes que conlleven altos riesgos similares.

La evaluación de impacto deberá efectuarse previo al inicio del tratamiento de datos personales mencionado en el presente artículo.

***Artículo 55. Notificación de vulneración de seguridad:*** El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales, dentro del término de tres (3) días a partir del conocimiento de dicha vulneración.

El encargado de tratamiento deberá notificar al responsable la vulneración de la seguridad de datos personales en un término no mayor a dos (2) días después de tener conocimiento de ella.

En caso de retraso del responsable o del encargado del tratamiento de datos personales en la notificación de vulneración de seguridad, sin que intermedie la debida justificación, se aplicarán las sanciones correspondientes, conforme a lo establecido en la presente ley.

En la notificación deberá constar lo siguiente:

1. La descripción de la naturaleza de la vulneración de la seguridad de los datos personales,
2. Las categorías y el número aproximado de titulares afectados;
3 Las categorías y el número aproximado de registros o campos de datos personales afectados;
4. El nombre y los datos de contacto del delegado de protección de datos, o a falta de este, de cualquier otro punto de contacto;
5. La descripción de las posibles consecuencias de la vulneración de la seguridad de los datos personales;
6. La descripción de las medidas adoptadas, implementadas o propuestas por el responsable para remediar la vulneración de la seguridad de los datos personales; y,
7 De ser el caso, las medidas adoptadas e implementadas para mitigar los posibles efectos negativos de la vulneración de la seguridad de datos personales.

Una vez tomado conocimiento de la vulneración de las seguridades de datos personales, el responsable deberá efectuar el análisis de riesgo sobre los derechos de libertad de sus titulares.

La notificación de las vulneraciones de seguridad de datos personales tendrá como objeto principal que la Autoridad de Protección de Datos Personales lleve un registro estadístico sobre vulneraciones e identificar posibles medidas de seguridad para cada una de ellas, así como identificar sectores o instituciones más vulnerables y promover nuevas regulaciones que busquen mejorar las seguridades exigibles a los responsables de tratamiento y otorgar seguridad jurídica en el tratamiento de datos personales

La Autoridad de Protección de Datos Personales sólo podrá sancionar al responsable o encargado del tratamiento, cuando la vulneración de seguridad de datos personales ha sido producto de incumplimientos a las medidas de seguridad adecuadas. En tal caso, la notificación oportuna de la violación por parte del responsable de tratamiento, tanto a la autoridad como al titular, así como las medidas de respuesta adoptadas, serán considerados como un atenuante de la infracción

En caso de no cumplimiento del término para la notificación, el responsable del tratamiento deberá justificar la dilación, caso contrario, se procederá conforme al régimen sancionatorio establecido para el efecto.

***Artículo 56. Acceso a datos personales para atención a emergencias e incidentes informáticos***: Las autoridades públicas competentes, los equipos de respuesta de emergencias informáticas, los equipos de respuesta a incidentes de seguridad informática, los centros de operaciones de seguridad, los prestadores y proveedores de servicios de telecomunicaciones y los proveedores de tecnología y servicios de seguridad, nacionales e internacionales, podrán acceder y efectuar tratamientos sobre los datos personales contenidos en las notificaciones de vulneración a las seguridades durante el tiempo y alcance necesarios para, de forma exclusiva, su detección, análisis, protección y respuesta ante incidentes, así como para adoptar e implementar medidas de seguridad adecuadas y proporcionadas a los riesgos identificados.

***Artículo 57. Notificación de vulneración de seguridad al titular***: El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a su titular, cuando conlleve un riesgo a sus derechos de libertad, de forma inmediata o hasta dentro de un término de tres (3) días, contados a partir de tener conocimiento del riesgo

No se deberá notificar al titular si se cumple alguna de las siguientes condiciones:

1. Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas, organizativas o de cualquier otra índole apropiadas, aplicadas a los datos personales afectados por la vulneración de su seguridad;
2. Cuando el responsable del tratamiento haya tomado medidas que garanticen que ya no se concrete el riesgo para los derechos de libertad del titular; y,
3. Cuando se requiera un esfuerzo desproporcionado, para lo cual se realizará una comunicación pública, a través de cualquier medio, en la que se informe a los titulares.

La notificación al titular del dato contendrá lo señalado en el artículo precedente

En caso de no cumplimiento del término para la notificación, el responsable del tratamiento deberá justificar la dilación, caso contrario, se procederá conforme al régimen sancionatorio establecido para el efecto.

***Artículo 58. Delegado de protección de datos personales***: Se designará un delegado de protección de datos personales cuando:

1 El tratamiento se lleve a cabo por quienes conforman el sector público de acuerdo con lo establecido en el artículo 225 de la Constitución de la República,
2 Las actividades del responsable o encargado de tratamiento de datos personales requieran de un control permanente y sistematizado debido a su volumen, naturaleza, alcance y/o finalidades del tratamiento,
3. Se refiera a tratamientos de gran volumen de categorías especiales de datos; y,
4. El tratamiento se refiera a datos relacionados con la seguridad nacional y defensa del Estado no regulado por normativa especializada.

La Autoridad de Protección de Datos Personales podrá definir nuevas condiciones para la necesidad de contar con un Delegado de Protección de Datos Personales, así como emitir directrices para su designación

***Artículo 59. Consideraciones especiales para el delegado de protección de datos personales***: Para la ejecución de sus funciones como delegado de protección de datos personales, se deberá considerar lo siguiente:

1. Corresponde al responsable y al encargado garantizar que la participación del delegado de protección de datos personales, en todas las cuestiones relativas a la protección de datos personales, sea apropiada y oportuna;
2. Es responsabilidad del responsable y del encargado facilitar el acceso a los datos personales y a las operaciones de tratamiento, así como todos los recursos y elementos necesarios para garantizar el correcto y libre desempeño de sus funciones,
3. Corresponde al responsable y al encargado capacitar y actualizar los conocimientos del delegado de protección de datos personales en la materia, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales;
4. El responsable y el encargado no podrán destituir o sancionar al delegado de protección de datos personales por el desempeño de sus funciones;
5. El delegado de protección de datos personales mantendrá relación directa con el más alto nivel jerárquico del responsable o encargado;
6. El titular podrá contactar al delegado de protección de datos personales en relación al tratamiento de sus datos personales y al ejercicio de sus derechos;
7 El delegado de protección de datos personales estará obligado a mantener la más estricta confidencialidad respecto a la ejecución de sus funciones; y,
8. Siempre que no exista conflicto con sus responsabilidades establecidas en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia, el delegado de protección de datos personales podrá desempeñar otras funciones dispuestas por el responsable o el encargado

***Artículo 60. Funciones del delegado de protección de datos personales:*** El delegado de protección de datos personales tendrá, entre otras, las siguientes funciones y atribuciones:

1 Informar y asesorar al responsable y encargado del tratamiento de datos personales, así como al personal relacionado al tratamiento de datos personales, respecto a las disposiciones contenidas en esta ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia,
2. Supervisar el cumplimiento de las disposiciones contenidas en esta ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia;
3. Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, así como supervisar su aplicación; y,
4. Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad en relación a las cuestiones referentes al tratamiento.

La Autoridad de Protección de Datos Personales podrá definir otras funciones, atribuciones y responsabilidades para el delegado de protección de datos personales, atendiendo a la naturaleza de los datos de carácter personal, al ámbito, el contexto y finalidades del tratamiento.

En caso de incumplimiento de sus funciones, responderá administrativa, civil y penalmente

## CAPÍTULO VII
## DE LA RESPONSABILIDAD PROACTIVA

***Artículo 61. Aplicación del principio de responsabilidad proactiva:*** Los responsables y encargados de tratamiento de datos personales podrán, de manera voluntaria, acogerse o adherirse a códigos de protección, estándares, certificaciones, sellos y mejores prácticas para dar cumplimiento al principio de responsabilidad proactiva, sin que esto constituya eximente de la responsabilidad de cumplir con las disposiciones de la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia.

La Autoridad de Protección de Datos Personales aprobará los contenidos de códigos de protección; evaluará, controlará, autorizará, sancionará y revocará, cuando sea procedente, las autorizaciones otorgadas a entidades certificadoras para su funcionamiento, así como evaluará, controlará y, de ser el caso, revocará las certificaciones y sellos otorgados por dichas entidades, y, además avalará estándares y mejores prácticas.

***Artículo 62. Atribuciones de las Entidades de Certificación:*** En materia de protección de datos personales, las Entidades de Certificación, podrán:

1. Emitir certificaciones de cumplimiento de la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y demás normativa sobre la materia;
2 Emitir sellos de protección de datos personales;
3. Llevar a cabo auditorías de protección de datos personales, y,
4. Certificar los procesos de transferencias internacionales de datos personales.

Los resultados de las auditorías podrán ser considerados como elementos probatorios dentro de los procesos sancionatorios.

***Artículo 63. Reconocimiento y revocatoria como Entidad Certificadora:*** La Autoridad de Protección de Datos Personales emitirá las directrices para la constitución y autorización de funcionamiento de las Entidades Certificadoras, y para su evaluación continua y permanente.

La Autoridad de Protección de Datos Personales, mediante resolución motivada, podrá revocar, de ser el caso, la autorización de funcionamiento como Entidad Certificadora en cualquier momento

## CAPÍTULO VIII
## TRANSFERENCIA O COMUNICACIÓN INTERNACIONAL DE DATOS PERSONALES

***Artículo 64. Transferencia o comunicación internacional de datos personales:*** La transferencia o comunicación internacional de datos personales será posible si se sujeta a lo previsto en el presente capítulo, la presente Ley o la normativa especializada en la materia, propendiendo siempre al efectivo ejercicio del derecho a la protección de datos personales

***Artículo 65. Criterios para declarar el nivel adecuado de protección:*** Para declarar de nivel adecuado de protección a países u organizaciones, la Autoridad de Protección de Datos Personales emitirá resolución motivada, en la cual se verificará la existencia de los siguientes presupuestos:

1. Que cuente con normativa que promueva y garantice el ejercicio de derechos fundamentales y libertades individuales;
2. Que cuente con una autoridad estatal independiente que garantice y promueva la efectiva tutela del derecho a la protección de datos personales;
3. Que cuente con normativa especializada en materia de protección de datos personales;
4. Que sea parte de Acuerdos o instrumentos internacionales vinculantes ratificados por un tercer país u organización que generen obligaciones respecto al tratamiento y trasferencia o comunicación de datos personales, siempre que estos establezcan un estándar igual o mayor de protección en favor del titular, más allá de su origen o nacionalidad, y,
5. Que posea legislación específica en materia seguridad nacional y defensa del Estado, que establezca mecanismos de control y verificación del acceso de las autoridades públicas a los datos personales de sus ciudadanos.

La resolución de nivel adecuado de protección deberá contemplar mecanismos de revisión periódica, al menos cada cinco años, para garantizar el derecho a la protección de datos personales. También establecerá acciones conjuntas entre las autoridades de ambos países con el objeto de prevenir, corregir o mitigar el tratamiento indebido de datos en ambos países

***Artículo 66. Transferencia o comunicación internacional de datos personales a países declarados como nivel adecuado de protección*:** Por principio general se podrán transferir o comunicar datos personales a países u organizaciones que brinden niveles adecuados de protección, conforme a los criterios establecidos en el artículo precedente.

***Artículo 67. Transferencia o comunicación mediante garantías adecuadas.*** Este mecanismo de transferencia o comunicación transfronteriza de datos personales opera cuando no existe una resolución de nivel adecuado de protección, en su lugar el responsable o encargado del tratamiento de datos personales deberá tomar medidas para compensar la falta de protección de datos en un tercer país u organización mediante garantías adecuadas para el titular, debiendo cumplir al menos con las siguientes.

1. Observancia de principios, derechos y obligaciones en el tratamiento de datos personales siempre que estos cumplan con un estándar igual o mayor de protección;
2 Efectiva tutela del derecho a la protección de datos personales, a través de la disponibilidad permanente de acciones administrativas o judiciales; y,
3 El derecho a solicitar la reparación integral, de ser el caso

Para la consecución de este mecanismo se requiere de instrumentos jurídicos vinculantes y exigibles entre autoridades y responsables del tratamiento de datos personales tales como: normas corporativas vinculantes, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas, códigos de protección, mecanismos de certificación, sellos de protección de datos personales aprobados

Corresponde a la Autoridad de Protección de Datos Personales dictar el contenido de las cláusulas estándar de protección de datos, así como la verificación de cláusulas o garantías adicionales o específicas acordadas entre las partes.

La Autoridad de Protección de Datos Personales aprobará códigos de protección, mecanismos de certificación y sellos de protección de datos personales

Para el cumplimiento de lo previsto en el presente artículo, se considerarán los derechos, garantías y principios de la presente ley, como requisitos y condiciones mínimas para la transferencia o comunicación internacional

***Artículo 68. Normas corporativas vinculantes***: Los responsables o encargados del tratamiento de datos personales podrán presentar a la Autoridad de Protección de Datos Personales normas corporativas vinculantes, específicas y aplicadas al ámbito de su actividad, en las cuales, para su aprobación, deberán cumplir las siguientes condiciones.

1. Ser de obligatorio cumplimiento para el responsable de tratamiento, la totalidad del grupo empresarial al que ésta pertenezca, sus empresas asociadas y cualquier otra empresa a la que eventualmente transfieran datos personales;
2. Brindar a los titulares los mecanismos adecuados para el ejercicio de sus derechos relacionados al tratamiento de sus datos personales, observando las disposiciones constantes en la presente ley;
3. Incluir una enunciación detallada de las empresas filiales que, además del responsable del tratamiento, pertenecen al mismo grupo empresarial. Además se incluirá la estructura y los datos de contacto del grupo empresarial o joint venture dedicadas a una actividad económica conjunta y de cada uno de sus miembros;
4. Incluir el detalle de las empresas encargadas del tratamiento de datos personales, las categorías de datos personales a ser utilizados, así como el tipo de tratamiento a realizarse y su finalidad;
5. Enunciar de forma expresa el carácter jurídicamente vinculante de tales normas a nivel nacional e internacional;
6. Observar en su contenido todas las disposiciones de la presente ley referentes a principios de tratamiento de datos personales, medidas de seguridad de datos, requisitos respecto a transferencia o comunicación internacional y transferencia o comunicación ulterior a organismos no sujetos a normas corporativas vinculantes;
7 Contener la aceptación por parte del responsable o del encargado del tratamiento de los datos personales o de cualquier miembro de su grupo empresarial sobre su responsabilidad por cualquier violación de las normas corporativas vinculantes. El responsable o encargado del tratamiento de datos personales no será responsable si éste demuestra que el acto que originó los daños y perjuicios no le es imputable.
8. Incluir los mecanismos en que se facilita al titular la información clara y completa, respecto a las normas corporativas vinculantes y sus efectos jurídicos;
9 Incluir las funciones de todo delegado de protección de datos designado o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o del joint venture dedicadas a una actividad económica conjunta bajo un mismo control, así como los mecanismos y procesos de supervisión y tramitación de reclamaciones,
10 Detallar los procesos o procedimientos en vía administrativa o judicial que le asistan;
11. Enunciar de forma detallada los mecanismos establecidos en el grupo empresarial o empresas afiliadas que permitan al titular verificar efectivamente el cumplimiento de las normas corporativas vinculantes. Entre estos mecanismos se incluirá auditorías continuas de protección de datos y aquellos métodos técnicos que brinden acciones correctivas para proteger los derechos del titular. Los resultados de las auditorías serán de acceso público, debidamente publicados y se pondrán a disposición de la Autoridad de Protección de Datos Personales en la periodicidad establecida en el reglamento a la presente ley;
12. Incluir los mecanismos para cooperar de forma coordinada con la Autoridad de Protección de Datos Personales y el responsable del tratamiento de los datos personales; y,

13 Incluir la declaración y compromiso del responsable del tratamiento de los datos personales de promover la protección de datos personales entre sus empleados con formación continua.

La Autoridad de Protección de Datos Personales definirá el formato y los procedimientos para la transferencia o comunicación de datos realizada por parte de los responsables, los encargados y las autoridades de control en lo relativo a la aplicación de las normas corporativas vinculantes a las que se refiere este artículo.

Cualquier cambio a ser realizado a estas normas deberá ser previamente aprobado por la Autoridad de Protección de Datos Personales y notificado al titular conforme a los mecanismos señalados por el responsable de tratamiento en su solicitud de aprobación.

***Artículo 69. Casos excepcionales de transferencias o comunicaciones internacionales***: En aquellos casos donde no se cumpla con los criterios de niveles adecuados de protección o de garantías adecuadas de protección, la Autoridad de Protección de Datos Personales podrá autorizar transferencias o comunicaciones internacionales de datos personales, en los siguientes casos:

1. A países u organismos internacionales que brinden garantías adecuadas para la protección de datos personales sin que necesariamente exista una ley específica o Autoridad de Protección de Datos Personales, para lo cual será necesaria la suscripción de un convenio o tratado internacional;
2. Cuando los datos personales sean requeridos para el cumplimiento de competencias institucionales, de conformidad con la normativa aplicable;
3. Cuando el titular haya otorgado su consentimiento explícito a la transferencia o comunicación propuesta, tras haber sido informado de las finalidades del tratamiento y posibles riesgos para él de dichas transferencias o comunicaciones internacionales, debido a la ausencia de una resolución de nivel adecuado de protección y de garantías adecuadas;
4. Cuando la transferencia internacional tenga como finalidad el cumplimiento de una obligación legal o regulatoria;
5 Cuando la transferencia internacional de datos personales sea necesaria para la ejecución de una obligación contractual entre el titular y el responsable del tratamiento de datos personales, o para la ejecución de medidas de carácter precontractual adoptadas a solicitud del titular;
6. Cuando la transferencia internacional de datos personales sea necesaria para la celebración o ejecución de un contrato, en interés del titular entre el responsable del tratamiento de datos personales y otra persona natural o jurídica;
7. Cuando la transferencia sea necesaria por razones de interés público;
8. Cuando la transferencia internacional sea necesaria para la colaboración judicial internacional,
9. Cuando la transferencia internacional sea necesaria para la cooperación dentro de la investigación de infracciones;
10. Cuando la transferencia internacional es necesaria para el cumplimiento de compromisos adquiridos en procesos de cooperación internacional entre Estados;
11. Transferencias bancarias y bursátiles;
12. Cuando la transferencia internacional de datos personales sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones, acciones administrativas o jurisdiccionales y recursos, y,
13. Cuando la transferencia internacional de datos personales sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento

***Artículo 70. Control continuo***: La Autoridad de Protección de Datos Personales en acciones conjuntas con la academia, realizará reportes continuos sobre la realidad internacional en materia de protección de datos personales. Dichos estudios servirán como elemento de control continuo del nivel adecuado de protección de datos personales de los países u organizaciones que ostenten tal reconocimiento.

En caso de detectarse que un país u organización ya no cumple con un nivel adecuado de protección conforme los principios, derechos y obligaciones desarrollados en la presente ley, la Autoridad de Protección de Datos Personales procederá a emitir la correspondiente resolución de no adecuación, a partir de la cual no procederán transferencias de datos personales, salvo que operen otros mecanismos de transferencia conforme lo dispuesto en el presente capítulo.

La Autoridad de Protección de Datos Personales publicará en cualquier medio, de forma permanente y debidamente actualizado, una lista de países, organizaciones, empresas o grupos económicos que garanticen niveles adecuados de protección de datos personales

## CAPITULO IX
## DE LAS OBLIGACIONES

***Artículo 71. Obligaciones del responsable del tratamiento de datos personales***: El responsable del tratamiento está obligado a.

1. Tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
2. Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia;
3. Aplicar e implementar procesos de verificación, evaluación y valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas;
4. Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular;
5. Adherirse a códigos de protección, mecanismos de certificación o sellos de protección de datos personales aprobados por la Autoridad de Protección de Datos Personales,
6. Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas;
7. Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;
8. Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas,
9. Notificar a la Autoridad de Protección de Datos Personales y al titular de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto;
10. Implementar la protección de datos personales desde el diseño y por defecto;
11. Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;

12. Elegir y designar el encargado del tratamiento de datos personales que ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme lo establecido en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional;
13. Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales;
14. Designar al Delegado de Protección de Datos Personales;
15 Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales; y,
16 Los demás establecidos en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

***Artículo 72. Obligaciones del encargado del tratamiento de datos personales***: El encargado del tratamiento de datos personales está obligado a·

1. Tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
2. Tratar datos personales de conformidad a lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales, inclusive en lo que respecta a la transferencia o comunicación internacional, salvo que esté obligado a hacerlo en función al principio de legitimidad; de ser este el caso, deberá informar al responsable del tratamiento de datos personales;
3. Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el personal a cargo del tratamiento de datos personales, o con quién tenga conocimiento de los datos personales;
4. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;
5. Implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales a efecto de evitar vulneraciones;
6. Asistir al responsable para que éste cumpla con su obligación de atender solicitudes que tengan por objeto el ejercicio de los derechos del titular frente al tratamiento de sus datos personales;
7. Asistir al responsable para garantizar el cumplimiento de las obligaciones previstas en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
8. Transferir o comunicar los datos personales entregados al responsable del tratamiento y suprimirlos, una vez que haya culminado su encargo;
9. Facilitar el acceso al responsable del tratamiento de datos personales de toda la información referente al cumplimiento de las obligaciones establecidas en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia,
10. Permitir y contribuir a la realización de auditorías o inspecciones, por parte del responsable del tratamiento de datos personales o de un auditor autorizado por éste o por la Autoridad de Protección de Datos Personales;
11. Cumplir el código de protección, mecanismos de certificación o sellos aprobados para demostrar la existencia de garantías suficientes para la protección de datos personales; y,

12. Las demás establecidas en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

## CAPITULO X
## DE LAS QUEJAS DIRECTAS Y DE LA GESTÍON DEL PROCEDIMIENTO ADMINISTRATIVO

***Artículo 73. Queja directa del titular del dato personal al responsable del tratamiento de datos personales:*** El titular de los datos personales podrá, en cualquier momento, de forma gratuita y por medios físicos o digitales puestos a su disposición por parte del responsable del tratamiento de los datos personales, presentar quejas sobre el contenido de los derechos, principios y obligaciones para hacer efectivas de forma directa sus peticiones, en especial aquellas relacionadas al acceso, rectificación o actualización, eliminación, oposición, limitaciones al tratamiento, portabilidad, notificaciones sobre violaciones a la seguridad, transferencia internacional a terceros países, entre otros.

Presentada la queja ante el responsable, este contará con un término de cinco (5) días para contestar y notificar en debida forma sobre su respuesta afirmativa o negativa, y ejecutar lo que se le haya solicitado.

***Artículo 74. Del inicio del procedimiento administrativo:*** La Autoridad de Protección de Datos Personales podrá iniciar de oficio o a petición del titular actuaciones previas, con el fin de conocer las circunstancias del caso concreto o la conveniencia o no de iniciar el procedimiento, para lo cual se estará conforme a las disposiciones del Código Orgánico Administrativo

***Artículo 75. Reclamo administrativo ante la Autoridad de Protección de Datos Personales:*** En el caso de que el responsable del tratamiento no conteste a la queja en el término establecido en la presente ley, o, ésta fuere negativa, el titular podrá presentar el correspondiente reclamo administrativo ante la Autoridad de Protección de Datos Personales, para lo cual se estará conforme al procedimiento establecido en el Código Orgánico Administrativo, la presente ley y demás normativa emitida por la Autoridad de Protección de Datos Personales

Sin perjuicio de lo antes expuesto, el titular podrá presentar acciones civiles, penales y constitucionales a las que se crea asistido.

## CAPÍTULO XI
## MEDIDAS CORRECTIVAS, INFRACCIONES Y RÉGIMEN SANCIONATORIO

***Artículo 76. Objeto y ámbito de aplicación:*** Los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, están sujetos a medidas correctivas, infracciones y al régimen sancionatorio establecido en el presente Capítulo.

En el caso de entidades pertenecientes al sector público, las resoluciones que determinen medidas correctivas o aplicación de régimen sancionatorio, deberán ser comunicada a la máxima autoridad de la institución responsable del tratamiento de datos personales con la finalidad de que se inicien los procedimientos disciplinarios en contra de los servidores o funcionarios, por cuya acción u omisión se hubiese incurrido en alguna de las infracciones establecidas en la presente ley, sin perjuicio de la responsabilidad civil, administrativa y/o penal a la que hubiere lugar.

***Artículo 77. Medidas correctivas***· En caso de incumplimiento de las obligaciones previstas en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia; o, transgresión a los derechos y principios que componen al derecho a la protección de datos personales, la Autoridad de Protección de Datos Personales dictará medidas correctivas con el objeto de reestablecer el derecho vulnerado y evitar que la conducta se produzca nuevamente, sin perjuicio de la aplicación de las correspondientes sanciones administrativas.

Las medidas correctivas podrán consistir, entre otras, en:

1. El cese del tratamiento bajo determinadas condiciones o plazos; y,
2. La imposición de medidas técnicas, jurídicas, organizativas o administrativas tendientes a garantizar un tratamiento adecuado de datos personales.

***Artículo 78. Implementación***: La Autoridad de Protección de Datos Personales, en el marco de esta ley, implementará para cada caso las medidas correctivas, previo informe de la unidad técnica competente, que permita corregir, revertir o eliminar las conductas contrarias a la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia.

Para la aplicación de las medidas correctivas se seguirán las siguientes reglas:

1. Para el caso de infracciones leves se aplicará a los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, únicamente medidas correctivas; en el caso de incumplimiento de dichas medidas correctivas o que éstas fueren cumplidas de forma tardía, parcial o defectuosa, la Autoridad de Protección de Datos Personales, aplicará las sanciones que corresponden a las infracciones leves establecidas en la presente ley.
2. En el caso de que los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, se encuentren incursos en el presunto cometimiento de una infracción leve y éstos consten dentro del Registro Único de Responsables y Encargados Incumplidos; la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida; y,
3 En el caso de que los responsables, encargados del tratamiento de datos personales y de ser el caso terceros, se encuentren incursos en el presunto cometimiento de una infracción grave, la Autoridad de Protección de Datos Personales activará directamente el procedimiento administrativo sancionatorio haciendo constar dentro de la resolución tanto las medidas correctivas aplicables como la sanción correspondiente a la infracción cometida

**Sección 1a**
**Del responsable**

***Artículo 79. Infracciones leves***. Se consideran infracciones leves las siguientes:

1. No tramitar, tramitar fuera del plazo previsto o negar injustificadamente las peticiones o quejas realizadas por el titular;

2. No notificar a la Autoridad de Protección de Datos Personales y al titular las vulneraciones de seguridad y protección de datos personales cuando no exista afectación a los derechos fundamentales y libertades individuales de los titulares;
3. No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales;
4 No mantener actualizado el Registro Nacional de Protección de Datos Personales de conformidad a lo dispuesto en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia; y,
5. Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales

***Artículo 80. Infracciones graves***: Se consideran infracciones graves las siguientes:

1 No implementar requisitos, mecanismos o herramientas administrativas, técnicas, físicas, organizativas y jurídicas a fin de garantizar que el tratamiento de datos personales se realice conforme la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
2. Utilizar información o datos para fines distintos a los declarados;
3. No cumplir lo dispuesto en códigos de protección, mecanismos de certificación, sellos de protección, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas y normas vinculantes;
4. Proceder a la comunicación de datos personales, sin cumplir con los requisitos y procedimientos establecidos en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
5. No utilizar metodologías de análisis y gestión de riesgos adaptadas a la naturaleza de los datos personales, las particularidades del tratamiento y de las partes involucradas;
6. No realizar evaluaciones de impacto al tratamiento de datos;
7. No implementar medidas técnicas, organizativas o de cualquier índole necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones a la seguridad de los datos personales que hayan sido identificadas;
8. No notificar a la Autoridad de Protección de Datos Personales y al titular las vulneraciones a la seguridad y protección de datos personales cuando afecte los derechos fundamentales y libertades individuales de los titulares;
9 No implementar protección de datos desde el diseño y por defecto,
10. No suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales;
11. Elegir al encargado del tratamiento de datos personales que no ofrezca garantías suficientes para hacer efectivo el ejercicio del derecho a la protección de datos personales;
12. No consignar en el Registro Nacional de Protección de Datos Personales lo dispuesto en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
13. No designar al Delegado de Protección de Datos Personales;
14. No permitir o no contribuir a la realización de auditorías o inspecciones, por parte del auditor acreditado por la Autoridad de Protección de Datos Personales, y,
15. El incumplimiento de las medidas correctivas o el cumplimiento de éstas de forma tardía, parcial o defectuosa; siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve.

**Sección 2ª**
**Del encargado**

***Artículo 81. Infracciones leves:*** Se consideran infracciones leves las siguientes:

1. No asistir al responsable para que éste cumpla con su obligación de atender solicitudes que tengan por objeto el ejercicio de los derechos del titular frente al tratamiento de sus datos personales.
2. No facilitar el acceso al responsable del tratamiento de datos personales a toda la información referente al cumplimiento de las obligaciones establecidas en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
3. No permitir o no contribuir a la realización de auditorías o inspecciones, por parte del responsable del tratamiento de datos personales o de otro auditor autorizado por éste o por la Autoridad de Protección de Datos Personales; y,
4. Incumplir las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales

***Artículo 82. Infracciones graves:*** Se consideran infracciones graves las siguientes:

1. No tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia;
2. No tratar datos personales de conformidad con lo previsto en el contrato que mantenga con el responsable del tratamiento de datos personales, inclusive en lo que respecta a la transferencia o comunicación internacional;
3. No suscribir contratos de confidencialidad y manejo adecuado de datos personales con el personal a cargo del tratamiento de datos personales, o quién tenga conocimiento de los datos personales;
4. No implementar mecanismos destinados a mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales;
5. No implementar medidas preventivas y correctivas en la seguridad de los datos personales a efecto de evitar vulneraciones;
6. No suprimir los datos personales transferidos o comunicados al responsable del tratamiento de los datos personales una vez haya culminado su encargo;
7. No cumplir lo dispuesto en códigos de protección, mecanismos de certificación, sellos de protección, cláusulas estándar de protección de datos, cláusulas o garantías adicionales o específicas y normas vinculantes;
8. Proceder a la comunicación de datos personales, sin cumplir con los requisitos y procedimientos establecidos en la presente ley, su reglamento, directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia, y,
9 El incumplimiento de las medidas correctivas o el cumplimiento de éstas de forma tardía, parcial o defectuosa, siempre y cuando hubiese precedido por dicha causa la aplicación de una sanción por infracción leve.

***Artículo 83. Sanciones por infracciones leves:*** La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas en el caso de verificarse el cometimiento de una infracción leve, según las siguientes reglas:

1. Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones leves establecidas en la presente Ley serán sancionados con una multa de uno (1) a diez (10) salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente
2. Si el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, es una entidad de Derecho Privado o una Empresa Pública se aplicará una multa de entre el 3% y el 9% calculada sobre su volumen de negocio, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad para lo cual deberá verificar los siguientes presupuestos·

    a) La intencionalidad, misma que se establecerá en función a la conducta del infractor;
    b) Reiteración de la infracción; es decir, cuando el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar,
    c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,
    d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar

***Artículo 84. Sanciones por infracciones graves***: La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas en el caso de verificarse el cometimiento de una infracción grave conforme a los presupuestos establecidos en el presente Capítulo:

1. Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente ley serán sancionado con una multa de entre diez (10) a veinte (20) salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente
2. Si el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, es una entidad de Derecho Privado o una Empresa Pública se aplicará una multa de entre el 10% y el 17% calculada sobre su volumen de negocio, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad para lo cual deberá verificar los siguientes presupuestos:

    a) La intencionalidad, misma que se establecerá en función a la conducta del infractor;
    b) Reiteración de la infracción, es decir, cuando el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero; hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;
    c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,

d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

En el caso de que el responsable, encargado del tratamiento de datos personales o un tercero de ser el caso; sea una organización sin domicilio ni representación jurídica en el territorio ecuatoriano, la Autoridad de Protección de Datos Personales notificará de la Resolución con la cual se establezca la infracción cometida a la autoridad de protección de datos, o quien hiciera sus veces, del lugar en donde dicha organización tiene su domicilio principal, a fin de que sea dicho organismo quien sustancie las acciones y/o procedimientos destinados al cumplimiento de las medidas correctivas y sanciones a las que hubiere lugar.

***Artículo 85. Sanciones por infracciones graves***: La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas en el caso de verificarse el cometimiento de una infracción grave conforme a los presupuestos establecidos en el presente Capítulo·

1. Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente Ley serán sancionado con una multa de entre 10 a 20 salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente.
2. Si el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero, es una entidad de Derecho Privado o una Empresa Pública se aplicará una multa de entre el 10% y el 17% calculada sobre su volumen de negocio, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad para lo cual deberá verificar los siguientes presupuestos.

   a) La intencionalidad, misma que se establecerá en función a la conducta del infractor;
   b) Reiteración de la infracción, es decir, cuando el responsable, encargado del tratamiento de datos personales y/o de ser el caso un tercero; hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;
   c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y,
   d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar.

En el caso de que el responsable, encargado del tratamiento de datos personales o un tercero de ser el caso; sea una organización sin domicilio ni representación jurídica en el territorio ecuatoriano, la Autoridad de Protección de Datos Personales notificará de la Resolución con la cual se establezca la infracción cometida a la autoridad de protección de datos, o quien hiciera sus veces, del lugar en donde dicha organización tiene su domicilio principal, a fin de que sea dicho organismo quien sustancie las acciones y/o procedimientos destinados al cumplimiento de las medidas correctivas y sanciones a las que hubiere lugar

***Artículo 86. Volumen de Negocio***: A efectos del Régimen Sancionatorio de la presente Ley, se entiende por volumen de negocio, a la cuantía resultante de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa

deducción del impuesto sobre el valor agregado y de otros impuestos directamente relacionados con la operación económica.

***Artículo 87. Medidas provisionales o cautelares:*** La Autoridad de Protección de Datos Personales podrá aplicar medidas provisionales de protección o medidas cautelares contempladas en la norma procedimental administrativa.

## CAPÍTULO XI
## AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

***Artículo 88. Autoridad de Protección de Datos Personales.*** La Autoridad de Protección de Datos Personales será una entidad de derecho público dependiente de la Función Ejecutiva con personería jurídica y gozará de autonomía administrativa y financiera.

***Artículo 89. Funciones, atribuciones y facultades:*** Corresponden a la Autoridad de Protección de Datos Personales las siguientes funciones, atribuciones y facultades

1. Ejercer la supervisión, control y evaluación de las actividades efectuadas por el responsable y encargado del tratamiento de datos personales y de las entidades certificadoras, de conformidad a lo establecido en la presente Ley, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales;
2. Conocer sobre los proyectos de normas de carácter general o técnico que se desarrollen en materia de protección de datos personales;
3. Emitir normativa general o técnica, criterios y demás actos que sean necesarios para el ejercicio de sus competencias y garantizar el ejercicio del derecho a la protección de datos personales.
4. Promover proyectos de ley o reformas en materia de protección de datos personales;
5. Autorizar y revocar la autorización de funcionamiento de entidades certificadoras, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;
6 Revisar, aprobar, rechazar, revocar y exigir la modificación de códigos de protección, mecanismos de certificación o sellos de protección de datos personales, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente;
7. Revocar las certificaciones o sellos de protección en materia de datos personales, conforme a los presupuestos establecidos en la normativa emitida para dicha finalidad y elaborar el modelo de gestión correspondiente,
8. Promover una coordinación adecuada y eficaz con entidades de certificación o agentes privados encargados de la rendición de cuentas, y participar en iniciativas internacionales y regionales para la protección de la protección de los datos personales;
9. Dictar las cláusulas estándar de protección de datos, así como verificar el contenido de las cláusulas o garantías adicionales o específicas,
10. Conocer, sustanciar y resolver los reclamos interpuestos por el titular o aquellos iniciados de oficio; así como aplicar las sanciones correspondientes,
11. Atender consultas en materia de protección de datos personales;
12 Promover e incentivar el ejercicio del derecho a la protección de datos personales,
13. Ejercer el control y emitir las resoluciones de autorización para la transferencia internacional de datos;

14. Coordinar con otros organismos del sector público y privado los esfuerzos para formular y aplicar planes y políticas destinados a fortalecer la protección de datos personales;
15 Ejercer la representación internacional en materia de protección de datos personales;
16. Coordinar, promover y ejecutar programas de cooperación con organismos internacionales análogos en materia de protección de datos personales, así como con unidades nacionales relacionadas, dentro del marco de sus competencias; y ejecutar acciones conjuntas a través de convenios de cooperación nacional o internacional;
17. Prestar asistencia en asuntos relacionados con la protección de datos personales a petición de un organismo nacional o internacional, de una entidad pública o privada;
18. Emitir directrices para el diseño y contenido de la política de tratamiento de datos personales;
19. Establecer directrices para el análisis, evaluación y selección de medidas de seguridad de los datos personales;
20. Llevar un registro estadístico sobre vulneraciones a la seguridad de datos personales e identificar posibles medidas de seguridad para cada una de ellas;
21. Solicitar información sobre su gestión a responsables, encargados y entidades de certificación para el cumplimiento de sus funciones de control y demás atribuciones establecidas en la presente ley;
22 Realizar o delegar auditorías técnicas al tratamiento de datos personales de conformidad a lo establecido en la presente Ley, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales;
23. Solicitar y recabar información para el análisis y elaboración de estudios en materia de protección de datos personales;
24. Publicar periódicamente una guía de la normativa relativa a la protección de datos personales;
25. Ejercer la potestad sancionadora respecto de responsables, encargados, terceros y entidades de certificación, conforme a lo establecido en la presente ley;
26. Crear, dirigir y administrar el Registro Nacional de Protección de Datos Personales, así como, coordinar las acciones necesarias con entidades del sector público y privado para su efectivo funcionamiento;
27 Promover la concientización en las personas y la compresión de los riesgos, normas, garantías y derechos en relación con el tratamiento y uso de sus datos personales, con especial énfasis en actividades dirigidas a grupos de atención prioritaria, tales como niñas, niños y adolescentes;
28. Compartir con organismos internacionales análogos en materia de protección de datos personales, así como con entidades nacionales e internacionales de control o fiscalización de índole administrativa o judicial: (i) informes, (ii) información; o (iii) datos personales relacionados a procesos de investigación, en el marco de sus competencias y de conformidad con la normativa aplicable, sin que dicha transferencia constituya una vulneración al principio de confidencialidad al constituir parte de la cadena de custodia, con la finalidad exclusiva de realizar el análisis, investigación y toma de acciones legales, judiciales y las demás que fueren pertinentes, pudiendo ser además utilizada como instrumento probatorio;
29 Controlar y supervisar el ejercicio del derecho a la protección de datos personales dentro del tratamiento de datos llevado a cabo a través del Sistema Nacional de Registros Públicos, y,
30 Las demás atribuciones establecidas en la normativa vigente.

***Artículo 90. Registro Nacional de Protección de Datos Personales:*** El responsable del tratamiento de datos personales deberá reportar a la Autoridad de Protección de Datos, lo siguiente

1 Identificación de la base de datos o del tratamiento;

2 El nombre, domicilio legal y datos de contactabilidad del responsable y encargado del tratamiento de datos personales;
3. Características y finalidad del tratamiento de datos personales;
4. Naturaleza de los datos personales tratados;
5. Identificación, nombre, domicilio legal y datos de contactabilidad de los destinatarios;
6. Modo de interrelacionar la información registrada,
7. Medios utilizados para implementar los principios, derechos y obligaciones contenidas en la presente ley y normativa especializada;
8 Requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales;
9 Tiempo de conservación de los datos;
10. Transferencias internacionales;
11. Constancia de la existencia de códigos de conducta; y,
12. Constancia de disponibilidad de certificaciones, sellos y marcas de protección de datos personales;

Este registro deberá mantenerse actualizado en todo momento, de esta manera se controlará que ningún responsable o encargado del tratamiento de datos personales, los trate con fines y características distintas a las declaradas en el registro o contrarias a la ley y normativa especializada en la materia.

## DISPOSICIONES GENERALES

***Primera:*** En lo dispuesto al procedimiento administrativo se estará a lo previsto en el Código Orgánico Administrativo

***Segunda:*** En el ámbito del derecho de acceso a la información pública son aplicables las disposiciones de las leyes de la materia.

***Tercera:*** En el ámbito de los datos personales registrables, son aplicables las disposiciones de las leyes de la materia.

***Cuarta:*** La Autoridad de Protección de Datos Personales será responsable de coordinar las acciones necesarias con entidades del sector público y privado para el efectivo funcionamiento del Registro Nacional de Protección de Datos Personales.

***Quinta:*** La Autoridad de Protección de Datos Personales será responsable de presentar informes bianuales de evaluación y revisión de la presente Ley, a la ciudadanía.

***Sexta:*** Créase el Registro Único de Responsables y Encargados Incumplidos, en el cual se llevará un registro de los Responsables y Encargados del Tratamiento de Datos Personales, que hayan incurrido en una de las infracciones establecidas en la presente Ley: mismo que tendrá fines sociales, estadísticos, preventivos y de capacitación, cuyo funcionamiento estará establecido en el Reglamento de la Ley de Protección de Datos Personales.

***Séptima:*** El ejercicio de los derechos reconocidos en la presente norma podrá ser exigido por el titular independientemente de la entrada en vigor del régimen sancionatorio.

## DISPOSICIONES TRANSITORIAS

***Primera:*** Las medidas correctivas y el régimen sancionatorio se aplicarán dentro de dos años contados a partir de la entrada en vigencia de la presente Ley, sin perjuicio de que en el transcurso de este tiempo los responsables y encargados del tratamiento se adecuen a los preceptos establecidos dentro de esta norma, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales.

***Segunda:*** Todo tratamiento realizado previo a la entrada en vigencia de la presente Ley deberá adecuarse a lo previsto en la presente norma dentro del plazo de dos años contados a partir de su publicación en el Registro Oficial.

El incumplimiento de la presente disposición dará lugar a la aplicación del régimen sancionatorio establecido en esta Ley.

***Tercera:*** Los responsables y encargados del tratamiento de datos personales que hayan implementado los preceptos recogidos dentro de esta Ley antes del plazo señalado en la Disposición Final Primera obtendrán un reconocimiento por buenas prácticas por parte de la Autoridad de Protección de Datos Personales.

***Cuarta:*** La transferencia internacional de datos personales que hubiere sido realizada antes de la entrada en vigencia de la presente Ley será legítima, sin perjuicio de que el responsable del tratamiento de datos personales deba aplicar lo dispuesto en esta norma para acreditar su responsabilidad proactiva y demostrada El responsable de tratamiento deberá adecuar la transferencia internacional de datos personales a la presente norma en un plazo no mayor de dos años contados a partir de la publicación de la presente norma en el Registro Oficial

El incumplimiento de la presente disposición dará lugar a la aplicación del régimen sancionatorio establecido en esta Ley.

## DISPOSICIONES REFORMATORIAS

***Primera:*** De la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el Suplemento del Registro Oficial 557 del 17 de abril de 2002:

1. Suprímase las definiciones de intimidad, datos personales, datos personales autorizados del glosario de términos establecido en la Disposición General Novena.

2 Sustitúyase el texto del artículo 32 por el siguiente: "Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales conforme a los presupuestos establecidos en la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación y demás normativa emitida por la Autoridad de Protección de Datos Personales"

***Segunda:*** Suprímase el inciso segundo del artículo 21 del Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicado en el Registro Oficial 735 del 31 de diciembre de 2002.

***Tercera:*** En la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicada en el suplemento del Registro Oficial 162 del 31 de marzo del 2010:

1 Sustitúyase:

a) El término Dirección Nacional de Registro de Datos Públicos por Dirección Nacional de Registros Públicos;

b) El término Sistema Nacional de Registro de Datos Públicos por Sistema Nacional de Registros Públicos;

c) El término Registro de Datos Públicos por Registros Públicos;

d) El término datos de carácter personal por datos personales;

e) El término dato público registral por la expresión datos públicos y datos personales registrables;

f) El artículo 6, por el siguiente: "Art. 6.- Accesibilidad y confidencialidad.- Son confidenciales los datos de carácter personal El acceso a estos datos, sólo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales.

Al amparo de esta Ley, para acceder a la información sobre el patrimonio de las personas cualquier solicitante deberá justificar y motivar su requerimiento, declarar el uso que hará del mismo y consignar sus datos básicos de identidad, tales como· nombres y apellidos completos, número del documento de identidad o ciudadanía, dirección domiciliaria y los demás datos que mediante el respectivo reglamento se determinen. Un uso distinto al declarado dará lugar a la determinación de responsabilidades, sin perjuicio de las acciones legales que el titular de la información pueda ejercer.

La Directora o Director Nacional de Registros Públicos, definirá los demás datos que integran el sistema nacional y el tipo de reserva y accesibilidad."

2. Incorpórese:

a) En el artículo 31 referente a las atribuciones y facultades de la Dirección Nacional de Registros Públicos antes del numeral 14 el siguiente:

"14. Controlar y supervisar que las entidades pertenecientes al Sistema Nacional de Registros Públicos incorporen mecanismos de protección de datos personales, así como dar cumplimiento a las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación y demás normativa que la Autoridad de Protección de Datos Personales dicte para el efecto;

15. Tratar datos procedentes del Sistema Nacional de Registros Públicos o de cualquier otra fuente, para realizar procesos de analítica de datos, con el objeto de prestar servicios al sector público, al sector privado y a personas en general, así como generar productos, reportes, informes o estudios, entre otros. Se utilizarán medidas adecuadas que garanticen el derecho a la protección de datos

personales y su uso en todas las etapas del tratamiento, como por ejemplo, técnicas de disociación de datos, y."

3. Suprímase del numeral 13 del artículo 31 lo siguiente: "y,".

4. Reenumerar el numeral 14 del artículo 31 por numeral "16".

***Cuarta:*** En el Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicado en el suplemento del Registro Oficial 718 del 23 de marzo del 2016:

Sustitúyase:

1 El término Dirección Nacional de Registros de Datos Públicos por Dirección Nacional de Registros Públicos;

2. El término Sistema Nacional de Registro de Datos Públicos por Sistema Nacional de Registros Públicos;

3. El término Registro de Datos Públicos por Registros Públicos;

4. El término datos de carácter personal por datos personales; y

5. El término dato público registral por la expresión datos públicos y datos personales registrables.

Incorpórese:

En la Disposición General Séptima el siguiente inciso final. "La definición de términos relacionados con el derecho a la protección de datos personales estará conforme a lo establecido en la ley de la materia."

***Quinta:*** En el Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, publicado en el suplemento del Registro Oficial 899 del 09 de diciembre de 2016, sustitúyase la palabra confidencialidad por protección en el numeral 5 del artículo 67.

***Sexta:*** En la Ley Orgánica de Telecomunicaciones, publicada en el tercer suplemento del Registro Oficial 439 del 18 de febrero de 2015:

1. Suprímase:
   a) El inciso, segundo, tercer y cuarto del artículo 79;

   b) En el primer inciso del artículo 83 lo siguiente: "(...) y seguridad de datos personales (. )"; y,

   c) En el inciso primero del artículo 85 lo siguiente: "(...) como de seguridad de datos personales (...)"

2. Sustitúyase:

   a) El artículo 78 por el siguiente:

**Art. 78. Seguridad de los Datos Personales:** Las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas, organizativas y de cualquier otra índole adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos personales de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales.

b) El artículo 81 por el siguiente:

**Art. 81. Guías telefónicas o de abonados en general:** Los abonados, clientes o usuarios tienen el derecho a no figurar en guías telefónicas o de abonados Deberán ser informados, de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales, de sus derechos con respecto a la utilización de sus datos personales en las guías telefónicas o de abonados y, en particular, sobre el fin o los fines de dichas guías, así como sobre el derecho que tienen, en forma gratuita, a no ser incluidos, en tales guías

c) El artículo 82 por el siguiente:

**Art. 82. Uso comercial de datos personales:** Las y los prestadores de servicios no podrán usar datos personales, información del uso del servicio, información de tráfico o el patrón de consumo de sus abonados, clientes o usuarios para la promoción comercial de servicios o productos, a menos que el abonado o usuario al que se refieran los datos o tal información, haya dado su consentimiento conforme lo establecido en la Ley Orgánica de Protección de Datos Personales. Los usuarios o abonados dispondrán de la posibilidad clara y fácil de retirar su consentimiento para el uso de sus datos y de la información antes indicada. Tal consentimiento deberá especificar los datos personales o información cuyo uso se autorizan, el tiempo y su objetivo específico

Sin contar con tal consentimiento y con las mismas características, las y los prestadores de servicios de telecomunicaciones no podrán comercializar, ceder o transferir a terceros los datos personales de sus usuarios, clientes o abonados. Igual requisito se aplicará para la información del uso del servicio, información de tráfico o del patrón de consumo de sus usuarios, clientes y abonados

d) El artículo 83 por el siguiente.

**Art. 83. Control técnico:** Cuando para la realización de las tareas de control técnico, ya sea para verificar el adecuado uso del espectro radioeléctrico, la correcta prestación de los servicios de telecomunicaciones, el apropiado uso y operación de redes de telecomunicaciones o para comprobar las medidas implementadas para garantizar el secreto de las comunicaciones y seguridad de datos personales, sea necesaria la utilización de equipos, infraestructuras e instalaciones que puedan vulnerar la seguridad e integridad de las redes, la Agencia de Regulación y Control de las Telecomunicaciones deberá diseñar y establecer procedimientos que reduzcan al mínimo el riesgo de afectar los contenidos de las comunicaciones.

Cuando, como consecuencia de los controles técnicos efectuados, quede constancia de los contenidos, se deberá coordinar con la Autoridad de Protección de Datos Personales para que:

a) Los soportes en los que éstos aparezcan no sean ni almacenados ni divulgados; y,
b) Los soportes sean inmediatamente destruidos y desechados

Si se evidencia un tratamiento ilegítimo o ilícito de datos personales, se aplicará lo dispuesto en la Ley Orgánica de Protección de Datos Personales.

***Séptima:*** En el Reglamento a la Ley Orgánica de Telecomunicaciones, publicado en el suplemento del Registro Oficial 676 del 25 de enero de 2016 sustitúyase:

1 El artículo 120, por el siguiente:

**Art. 120. Protección de datos personales:** Los prestadores de servicios del régimen general de telecomunicaciones tienen prohibido ejecutar u omitir acciones que violen la garantía de protección de datos personales, como por ejemplo, provocar la destrucción, la pérdida, la alteración, la revelación o el acceso no autorizado de datos personales, transmitidos, almacenados o tratados en la prestación de servicios de telecomunicaciones, conforme el alcance, los procedimientos o protocolos previstos en la Ley Orgánica de Protección de Datos Personales, su Reglamento y las resoluciones emitidas por la Autoridad de Protección de Datos Personales, para el efecto La violación de esta garantía dará lugar a la imposición de las sanciones previstas en el ordenamiento jurídico

2. El artículo 121, por el siguiente:

**Art. 121. Uso comercial:** Los datos personales que los usuarios proporcionen a los prestadores de servicios del régimen general de telecomunicaciones no podrán ser usados para la promoción comercial de servicios o productos, inclusive de la propia operadora; salvo consentimiento del usuario, de conformidad con lo establecido en la Ley Orgánica de Protección de Datos Personales.

Para tal fin, los prestadores de servicios deberán solicitar a sus usuarios su consentimiento, conforme lo establece la Ley Orgánica de Protección de Datos Personales, en un instrumento separado y distinto al contrato de prestación de servicios a través de medios físicos o electrónicos, para que la prestadora de servicios del régimen general de telecomunicaciones pueda utilizar comercialmente sus datos personales. Dicho instrumento debe contener lo determinado en la Ley Orgánica de Protección de Datos Personales, su Reglamento o las resoluciones que su Autoridad de Protección de Datos Personales, dicte para el efecto. Sin perjuicio de lo anterior se considerarán públicos los datos contenidos en las guías telefónicas de telefonía fija, no obstante lo cual los abonados tendrán derecho a que se excluyan gratuitamente sus datos personales de dichas guías.

La ARCOTEL establecerá los mecanismos y emitirá las regulaciones correspondientes a fin de precautelar el secreto de las comunicaciones y de la información que se trasmite a través de redes de telecomunicaciones, así como la seguridad de las redes.

***Octava:*** Sustitúyase del Capítulo III, del Título XIII, del Libro I, de la Resolución No. SB-2017-810, de 31 de Octubre 2017, que Codifica las Normas de la Superintendencia de Bancos:

El artículo 14, literal b por el siguiente: Las entidades financieras al tratar datos personales deberán apegarse a lo previsto en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y la normativa especializada emanada por la Autoridad de Protección de Datos Personales que dicte para el efecto.

## PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR

### DISPOSICIONES DEROGATORIAS

***Primera:*** Deróguese el artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, publicada en el suplemento del Registro Oficial 557 del 17 de abril de 2002.

***Segunda:*** Deróguese los artículos 80, y 84 de la Ley Orgánica de Telecomunicaciones, publicada en el tercer suplemento del Registro Oficial 439 del 18 de febrero de 2015.

***Tercera:*** Deróguese el artículo 5 de la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicada en el suplemento del Registro Oficial 162 del 31 de marzo del 2010.

***Cuarta:*** Deróguense los artículos 11 y 12 y los numerales 2, 3, 4, 5, 8, 10, 11, y 12 de la Disposición General Séptima del Reglamento a la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos publicado en el suplemento del Registro Oficial 718 del 23 de marzo del 2016.

***Quinta:*** Quedan así mismo derogadas todas aquellas disposiciones de igual o menor jerarquía que se contrapongan con la presente Ley Orgánica.

Dado en

FS

REPÚBLICA DEL ECUADOR
**ASAMBLEA NACIONAL**

ASAMBLEA NACIONAL
República del Ecuador

# Trámite 254848
Código validación 2FQYD4HAAQ
Tipo de documento OFICIO
Fecha recepción 12-jul-2016 18:14
Numeración documento pan-gr-2016-1692
Fecha oficio 12-jul-2016
Remitente RIVADENEIRA BURBANO GABRIELA ALEJANDRA
Función remitente PRESIDENTA
Revise el estado de su trámite en:
http://tramites.asambleanacional.gob.ec/dts/estadoTramite.jsf

**Oficio No. PAN-GR-2016-1692**
Quito, 12 de julio de 2016

Señora Doctora
Rosana Alvarado
**PRIMERA VICEPRESIDENTA DE LA ASAMBLEA NACIONAL**
En su despacho.-

De mi consideración:

De conformidad con la Ley Orgánica de la Función Legislativa, publicada en el Registro Oficial Nro. 63 de 10 de noviembre de 2009, artículo 54 numeral 1), que establece que la iniciativa para presentar los proyectos de ley corresponde a los asambleístas con el apoyo de una bancada legislativa o de al menos el cinco por ciento de sus miembros, me permito presentar, en calidad de asambleísta nacional, el Proyecto de Ley Orgánica de la Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales.

Este Proyecto cuenta con el respaldo necesario para el tratamiento en el Pleno de la Asamblea Nacional.

Atentamente,

Gabriela Rivadeneira Burbano
**PRESIDENTA DE LA ASAMBLEA NACIONAL**

*UTL - CE*

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

# EXPOSICIÓN DE MOTIVOS

En el contexto de la era informacional, cada día se registran millones de datos bajo distintos procedimientos. Estos se gestionan y se encuentran expuestos al público. A pesar de la existencia de una normativa internacional y nacional dirigida a la protección de la privacidad e intimidad de las personas, los riesgos surgidos del desarrollo y la expansión de las nuevas tecnologías de la información y la comunicación elevan la vulnerabilidad de las personas en el tratamiento de su información personal. Por lo tanto, se impone la necesidad de una regulación del uso público y privado de la información personal y un proceso de concienciación de la colectividad sobre la misma.

La mayoría de las actividades sociales demandan un intercambio de información y su debida sistematización: abrir una cuenta en el banco, participar en un concurso, reservar un vuelo o un hotel, efectuar un pago con tarjeta de crédito o navegar en internet. Basta con *googlear* el nombre de una persona para tener acceso a los datos sobre su estado civil, cuenta telefónica, el objeto de su negocio u otro aspecto de su vida personal. Nombres y apellidos; fecha de nacimiento; dirección domiciliaria o de correo electrónico; número de identificación; matrícula del auto y muchos otros datos que se usan a diario, constituyen información que podría permitir identificar a una persona, ya sea directa o indirectamente. Estos datos que dicen mucho sobre nosotros, nuestra vida y nuestra intimidad personal están expuestos al libre acceso; carecen de protección y pueden ser utilizados para múltiples fines, no siempre lícitos.

El entorno digital es dinámico y es necesario responder con ritmo similar y con adaptación al ordenamiento jurídico para alcanzar que, en este contexto, los derechos de los individuos sean protegidos y garantizados y por lo tanto no se vean afectados. Si bien es cierto, la Constitución de 2008 garantiza el derecho a la intimidad personal y familiar (artículo 66), en la práctica, se ha vuelto relativamente simple acceder a la información personal, que solo debería ser proporcionada por el titular.

Ante la existencia de bases de datos públicas y privadas a través de las cuales se comercializa y difunde información personal, es indispensable una ley que ampare la decisión de las personas sobre sus datos y proteger su privacidad e intimidad, tanto en la esfera de su vida individual como familiar, dando especial relevancia a los derechos de los más vulnerables: niñas, niños y adolescentes.

Los datos personales, como se ha señalado anteriormente, dicen todo sobre la vida privada e íntima de la persona y pueden revelar la identidad, en consecuencia, deben ser protegidos. El libre acceso a la información puede vulnerar derechos e incidir negativamente en el bienestar, seguridad personal y familiar y por esto, la necesidad de regular la captación, aprovechamiento y flujo de la información personal.

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

La Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales que se propone, da repuesta a la problemática ocasionada en el tratamiento de datos personales en una era en la que los medios tecnológicos para su procesamiento y almacenamiento se desarrollan constantemente. Esta Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales apela al derecho fundamental que tienen las personas para disponer y decidir sobre toda la información relativa a su privacidad e intimidad.

La protección de datos para que sea integral, debe actuar en dos sentidos: por un lado, establecer los derechos del titular, como son otorgar y revocar el consentimiento del uso de su información personal, actualizarla y rectificarla; y, por otro, establecer las regulaciones en el procesamiento y tratamiento de la información personal por parte de entidades públicas y privadas cuya finalidad sea exclusivamente financiera o mercantil.

Esta Ley Orgánica de Protección de los Derechos a la Intimidad y Privacidad sobre los Datos Personales surge sobre la base del principio de autonomía de la persona, mediante la cual se establece un marco de regulación para la administración y gestión de los datos personales.

## LA ASAMBLEA NACIONAL

## EL PLENO

## CONSIDERANDO

Que el artículo 12 de la Declaración Universal de los Derechos Humanos dispone que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación";

Que el artículo 17 numeral 1 del Pacto Internacional de Derechos Civiles y Políticos establece que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y reputación; y, su numeral 2 determina que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques";

Que el artículo 11 numeral 2 de la Convención Interamericana sobre Derechos Humanos determina que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; y su numeral 3, sostiene que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques";

Que el artículo 66 numeral 3 de la Constitución de la República, garantiza el derecho a la integridad personal que incluye la integridad física, psíquica, moral y sexual;

Que el artículo 66 numeral 19 de la Norma Suprema "garantiza el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de ese carácter, así como la correspondiente protección";

Que el artículo 66 numeral 20 de la Norma Suprema "garantiza el derecho a la intimidad personal y familiar";

Que le artículo 6 de la Ley Orgánica de Garantías Constitucionales y Control Constitucional dispone que "las garantías jurisdiccionales tienen como finalidad la protección eficaz e inmediata de los derechos reconocidos en la Constitución y en los instrumentos internacionales de derechos humanos, la declaración de la violación de uno o varios derechos, así como la reparación integral de los daños causados por su violación";

Que el artículo 2 literal d) de la Ley Orgánica de Transparencia y Acceso a la Información Pública "garantiza la protección de la información personal en poder del sector público y/o privado";

Que el artículo 78 de la Ley Orgánica de Comunicación establece que "para la plena vigencia del derecho a la intimidad, establecido en el artículo 66, numeral 20, de la Constitución de la República, las y los prestadores de servicios de telecomunicaciones deberán garantizar, en el ejercicio de su actividad, la protección de los datos de carácter personal";

Que el artículo 53 del Código de la Niñez y Adolescencia dispone que "sin perjuicio de la natural vigilancia de los padres y maestros, los niños, niñas y adolescentes tienen derecho a que se respete la intimidad de su vida privada y familiar; y la privacidad e inviolabilidad de su domicilio, correspondencia y comunicaciones telefónicas y electrónicas, de conformidad con la ley. Se prohíbe las injerencias arbitrarias o ilegales en su vida privada";

Que el artículo 4 de la Ley del Sistema Nacional de Registro de Datos Públicos dispone que "las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo";

Que el artículo 6 de la Ley del Sistema Nacional de Registro de Datos Públicos manifiesta que "son confidenciales los datos de carácter personal, tales como: ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales";

Que el artículo 9 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos "determina que para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de estos, quien podrá seleccionar la información a compartirse con terceros";

Que el artículo 178 del Código Orgánico Integral Penal tipifica el delito de violación a la intimidad y determina que "la persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años";

Que el artículo 229 del Código Orgánico Integral Penal tipifica el delito de revelación ilegal de base de datos y determina que "la persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años"; y,

Que el artículo 475 numeral 1 del Código Orgánico Integral Penal establece que "la correspondencia física, electrónica o cualquier otro tipo o forma de comunicación, es inviolable, salvo los casos expresamente autorizados en la Constitución y en este Código".

Por lo expuesto, la Asamblea Nacional, en ejercicio de sus atribuciones constitucionales y legales, expide la siguiente:

# LEY ORGÁNICA DE PROTECCIÓN DE LOS DERECHOS A LA INTIMIDAD Y PRIVACIDAD SOBRE LOS DATOS PERSONALES

## TÍTULO I

## GENERALIDADES

**Artículo 1.- Objeto.** La presente Ley tiene por objeto proteger y garantizar el derecho de todas las personas a la intimidad y privacidad en el tratamiento de datos personales que se encuentren en bases o bancos de datos, ficheros, archivos, en forma física o digital, en instancias públicas o privadas.

**Artículo 2.- Ámbito de aplicación.** Los principios y disposiciones contenidas en la presente Ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada, en todo el territorio nacional.

Las limitaciones a los principios y derechos previstos en esta Ley, en cuanto a su observancia y ejercicio, corresponderán a la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.

**Artículo 3.- Principios generales.** Todos los involucrados en la formación, administración y manejo de bases o bancos de datos, ficheros, archivos, en forma física y/o digital, o que tengan relación con datos personales de terceros, están obligados a observar y respetar los siguientes principios:

1. **Legalidad:** la formación de bases de datos será lícita cuando se encuentren debidamente inscrita y la información haya sido obtenida por medios legítimos, en estricta observancia a la normativa en el ámbito relativo a esta materia.
2. **Pertinencia:** los datos personales no podrán ser utilizados para fines distintos a los que motivaron su obtención.
3. **Veracidad:** la recolección de datos personales deberá ser veraz y no excesiva; no podrá obtenerse por medios fraudulentos, abusivos o en forma contraria a la presente Ley.
4. **Consentimiento informado:** el titular de los datos deberá prestar su consentimiento libre, expreso, previo e informado para la entrega de los mismos. Se exceptúan los datos que provengan de fuentes públicas de información; se recaben para el ejercicio de funciones propias de las instituciones del Estado; deriven de relaciones contractuales, científicas o profesionales del titular de los datos y sean necesarias para su cumplimiento; y, se realicen por personas naturales para su uso exclusivo personal o doméstico.
5. **Confidencialidad:** tanto el responsable como el usuario de bases de datos debe adoptar medidas para resguardar de manera confidencial los datos personales, con el objeto de evitar su adulteración, pérdida o tratamiento no autorizado. Adicionalmente, los datos deberán ser almacenados de forma que permitan el acceso al titular.
6. **Reserva:** las personas naturales o jurídicas que obtengan legítimamente información proveniente de una base de datos están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de sus actividades, siendo prohibida la difusión a terceros.

**Artículo 4.- Definiciones.** Para los efectos de la presente Ley se entiende por:

1. **Base o banco de datos:** conjunto organizado de datos personales que es objeto de tratamiento o procesamiento, digital o no, cualquiera que sea la modalidad de su formación, almacenamiento, organización o acceso.

2. **Consentimiento del titular**: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular autoriza el tratamiento de datos personales.
3. **Dato personal:** cualquier información vinculada o que pueda asociarse a una o varias personas naturales identificadas o identificables: nombre y apellido, fecha de nacimiento, dirección domiciliaria, correo electrónico, número de teléfono, número de cédula, matrícula vehicular, información patrimonial e información académica o cualquier otra información vinculada con la identidad del titular.
4. **Datos sensibles:** datos que se refieren a las características físicas de la persona que revelan el origen racial y étnico, las convicciones ideológicas, filosóficas o morales, las opiniones políticas, creencias religiosas, los datos genéticos, la información referente a la salud y a la vida sexual o cualquier otro dato vinculado con la intimidad del titular.
5. **Disociación de datos**: procedimiento mediante el cual los datos personales no puedan vincularse a una persona determinada o determinable.
6. **Protección de datos personales:** facultad que otorga la Ley para que el dueño de los datos personales, decida a quién proporciona su información, cómo y para qué. Este derecho permite acceder, rectificar, cancelar y oponerse al tratamiento de su información personal.
7. **Responsable del tratamiento de la información:** persona natural o jurídica, pública o privada que sola o conjuntamente con otros, administra el sistema de tratamiento de datos personales por cuenta del responsable del archivo, registro, base o banco de datos. Toda operación de información que comprometa datos personales, en procedimiento mecánico o automatizado que tenga como fin la *recolección, ordenamiento, conservación,* almacenamiento, modificación, evaluación, destrucción, procesamiento de datos, así como el acceso de terceros por cualquier medio, deberá observar estrictamente la normativa prevista, bajo los derechos de protección y salvaguardia de identidad.
8. **Responsable del archivo, registro, base o banco de datos:** persona natural o jurídica, pública o privada que es titular de un archivo, registro, base o banco de datos como custodio y operador de la información.
9. **Titular de los datos:** persona natural cuyos datos personales son objeto de tratamiento.
10. **Tratamiento de datos:** cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, selecciona, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal o utilizarlos en cualquier otra forma.
11. **Usuario de datos:** persona natural o jurídica, pública o privada, que realiza el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos.

**Artículo 5.-Tratamiento de datos sensibles.** Se prohíbe el tratamiento de datos sensibles en todo aquello que pueda afectar el derecho a la intimidad de la persona. Nadie podrá ser obligado a proporcionar datos sensibles, salvo las siguientes circunstancias:

1. El titular autoriza expresamente y por escrito el tratamiento de datos sensibles.

2. El tratamiento es necesario para salvaguardar el interés vital del titular si este se encuentra física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

3. El tratamiento se refiere a datos que son indispensables para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

4. El tratamiento tiene una finalidad estadística, científica o académica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

## TÍTULO II

## DERECHOS Y OBLIGACIONES EN LA PROTECCIÓN DE DATOS

**Artículo 6.- Derechos de los Titulares.** El titular de los datos personales tendrá los siguientes derechos:

1. Conocer, actualizar y rectificar sus datos personales frente a los responsables o encargados del tratamiento.

2. Ser informado por el responsable o el encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.

3. Acceder en forma gratuita a sus datos personales que han sido objeto de tratamiento en instancias públicas y privadas.

4. Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando exista orden de autoridad competente.

5. Revocar el consentimiento, oponerse y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales, previo el trámite legal pertinente.

6. Presentar reclamos por incumplimiento a lo dispuesto en la presente Ley.

**Artículo 7.- Derechos de las niñas, niños y adolescentes.** Se asegurará el respeto al derecho a la intimidad de las niñas, niños y adolescentes, por lo que se prohíbe el

tratamiento de sus datos personales, salvo aquellos datos que sean de naturaleza pública. Es deber del Estado y de las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan las niñas, niños y adolescentes respecto del tratamiento indebido de sus datos personales; y, proveer de conocimiento acerca del uso responsable y seguro por parte de niñas, niños y adolescentes de sus datos personales, su derecho a la intimidad y protección de su información personal y a la de los demás.

**Artículo 8.- Obligaciones del responsable del tratamiento de la información.** Constituyen obligaciones del responsable del tratamiento de la información, las siguientes:

1. Requerir y obtener el consentimiento del titular de los datos personales, previo a su obtención y tratamiento.
2. Informar al titular de los datos, en forma expresa y clara, previamente a recabar información referida a su persona, acerca de:

   a) La existencia del archivo, registro, base o banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.

   b) La finalidad para la que serán tratados y quienes pueden ser sus destinatarios o categorías de destinatarios.

   c) El carácter obligatorio o facultativo de la respuesta a las preguntas que le sean formuladas.

   d) Las consecuencias que se deriven por proporcionar los datos, por la negativa a hacerlo o por la inexactitud de los mismos.

   e) La facultad y modo de ejercer los derechos de acceso, rectificación, actualización y supresión de los datos que le confiere la presente Ley.

3. Respetar en todo momento los principios generales de la protección de datos personales.
4. Proceder en forma inmediata a la rectificación, actualización o supresión, de los datos personales cuando fueran total o parcialmente inexactos, incompletos o desactualizados.
5. Inscribir sus archivos, registros, bases o bancos de datos en el Registro Nacional de Bases de Datos creado por el organismo de control.

**Artículo 9.- Obligaciones del responsable de las bases o bancos de datos, ficheros, archivos.** Le corresponde al responsable de las bases o bancos de datos, ficheros o archivos cumplir con las mismas obligaciones exigidas al responsable del tratamiento de la información tanto respecto de la confidencialidad y reserva que debe mantener sobre la

información obtenida, como del respeto y cumplimiento de los principios generales de la protección de datos personales.

El encargado de las bases de datos solo actuará según las instrucciones del responsable del tratamiento de datos y no podrá, bajo ningún concepto, ceder los datos personales sometidos a tratamiento, ni aun para su conservación.

**Artículo 10.- Obligaciones del usuario de datos.** Todas las personas que actúen, trabajen, o presten servicios de cualquier tipo en o para algún órgano del sector público o privado, solo podrán tratar los datos personales incorporados en las bases o bancos de datos, ficheros, archivos, de titularidad del órgano para o en el que desempeñen su tarea, cuando así lo disponga el responsable del tratamiento de la información en virtud de una obligación legal.

Quedan sujetos, al igual que los encargados del tratamiento, a los mismos deberes y obligaciones exigidos al responsable de las bases o bancos de datos, ficheros, archivos, tanto respecto de la confidencialidad y reserva que debe mantener sobre la información obtenida, como del respeto y cumplimiento a los principios generales de la protección de datos personales.

El usuario de datos solo podrá ceder los datos personales sometidos a tratamiento siguiendo expresas instrucciones del responsable del tratamiento.

## TÍTULO III

## TUTELA DE DERECHOS

**Artículo 11.- Autoridad Nacional de Protección de Datos Personales.** La Dirección Nacional de Registro de Datos Públicos adscrita al Ministerio de Telecomunicaciones y Sociedad de la Información será la Autoridad Nacional de Protección de Datos Personales y ejercerá la vigilancia y control para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley.

**Artículo 12.- Atribuciones de la Autoridad Nacional de Protección de Datos Personales.** Además de las atribuciones señaladas en otros cuerpos legales, la Dirección Nacional de Registro de Datos Públicos ejercerá las siguientes:

1. Velar por el cumplimiento de la legislación en materia de protección de datos personales.
2. Promover y divulgar los derechos de las personas en relación con el tratamiento de datos personales e implementar mecanismos de difusión acerca del ejercicio y garantía del derecho constitucional de la protección de datos.

3. Disponer el bloqueo temporal o definitivo de los sistemas de información cuando exista un riesgo cierto de afectación de derechos constitucionales, en caso de incurrir en infracciones contempladas en esta ley.
4. Solicitar a los responsables del tratamiento y responsables de las bases o bancos de datos, ficheros, archivos, la información necesaria para el ejercicio efectivo de sus funciones.
5. Realizar las declaraciones sobre las transferencias internacionales de datos, ejercer el control y adoptar las autorizaciones que procedan en relación con estas transferencias y cooperar en materia de protección internacional de datos personales.
6. Implementar un sistema de resguardo de la información para evitar su deterioro o desaparición.
7. Crear un Registro Nacional de Bases de Datos Personales y emitir las órdenes y los actos necesarios para su administración y funcionamiento.
8. Determinar la responsabilidad de las infracciones e imponer las sanciones a los responsables del tratamiento y responsables de las bases o bancos de datos, ficheros y archivos, previo el debido proceso correspondiente.
9. Realizar la vigilancia y control de las bases o bancos de datos, ficheros o archivos físicas o digitales.
10. Realizar campañas de concientización a la población sobre la necesidad de protección de datos personales y sensibles.
11. Las demás que le sean designadas por ley.

**Artículo 13.- Tutela de los derechos.** Las actuaciones contrarias a lo dispuesto en la presente ley serán objeto de acción constitucional de *habeas data*, conforme con lo establecido en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.

## TÍTULO IV

## REGISTRO NACIONAL DE BASES DE DATOS PERSONALES

**Artículo 14.- Definición.** El Registro Nacional de Bases de Datos Personales es el conjunto organizado de bases o bancos de datos, ficheros, archivos, en forma física o digital, de instancias públicas o privadas, que operan en el país, sujetos a tratamiento.

**Artículo 15.- Administración.** El Registro será administrado por la Autoridad Nacional de Protección de Datos Personales.

**Artículo 16.- Inscripción registral.** Todas las base o bancos de datos, ficheros o archivos, en forma física o digital, de instancias públicas y las base o bancos de datos, ficheros, o archivos, en forma física o digital de empresas e instituciones privadas con fines exclusivamente financieros y mercantiles deberán inscribirse en el Registro Nacional de

Bases de Datos Personales de acuerdo con los procedimientos y criterios que la Dirección Nacional de Registro de Datos Públicos establezca para el efecto

**Artículo 17.- Tratamiento de datos efectuado por terceros.** Si el responsable de archivo, registro, base de datos debe encargar a un tercero este servicio, requerirá de autorización expresa de la autoridad competente para que se realice el respectivo control.

**Artículo 18.- Requisitos para la inscripción**. Las bases o bancos de datos, ficheros, archivos, en forma física o digital, en instancias públicas o privadas, para su inscripción en el Registro Nacional de Bases de Datos, deberán contener:

1. Identificación de la base de datos y el responsable de la misma.
2. Naturaleza de los datos que contiene.
3. Procedimientos de obtención y tratamientos de los datos.
4. Medidas de seguridad y descripción técnica de la base de datos.
5. Declaración sobre la protección de datos personales.
6. Destino de los datos y personas físicas o jurídicas a las que puedan ser transmitidos.
7. Tiempo de conservación de los datos.
8. Forma y condiciones en que las personas pueden acceder a los datos.
9. Procedimientos para la rectificación o actualización de los datos.

El incumplimiento de estos requisitos dará lugar a la sanción prevista en esta Ley.

**Artículo 19.- Autorización de Operaciones.** Las bases o bancos de datos, ficheros, archivos, en forma física o digital provenientes del sector privado, para ejecutar sus actividades, además de la inscripción obligatoria en el Registro Nacional de Bases de Datos contarán con una autorización de operaciones.

La Autoridad Nacional de Protección de Datos Personales establecerá mediante reglamento los requisitos y procedimientos para la obtención de la autorización.

## TÍTULO V

## TRANSFERENCIA INTERNACIONAL DE DATOS

**Artículo 20.- Prohibición.** Se prohíbe la transferencia de datos personales de cualquier tipo a países u organismos internacionales que no proporcionen niveles de protección de datos, conforme con las normas de derecho internacional o regional en la materia.

**Artículo 21.- Excepciones.** La prohibición a la que se refiere el artículo anterior no será de aplicación en los siguientes casos:

1. Cuando el titular haya otorgado su autorización expresa e inequívoca para la transferencia de datos personales.
2. Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico.
3. Cuando se refiera a transferencias bancarias o bursátiles, conforme con la legislación aplicable.
4. Cuando la transferencia internacional de datos resulte de la aplicación de tratados o convenios internacionales en los cuales Ecuador sea parte, con fundamento en el principio de reciprocidad.
5. Cuando la transferencia sea necesaria o legalmente exigida para salvaguardar el interés público.
6. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
7. Cuando la transferencia sea necesaria para la ejecución de un contrato entre el titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del titular.

## TÍTULO VI

## INFRACCIONES Y SANCIONES

**Artículo 22.- Responsabilidad.** Sin perjuicio de incurrir en infracciones penales, en caso de incumplimiento con lo previsto sobre la protección de datos personales, los responsables de tratamiento, los responsables de las bases o bancos de datos, ficheros, archivos, en forma física o digital y los usuarios, en instancias públicas y privadas, estarán sujetos al régimen sancionatorio, conforme con el presente Título.

**Artículo 23.- Clasificación de las infracciones**. Según su magnitud e importancia, las infracciones se clasifican en leves y graves.

**Artículo 24.- Infracciones leves.** Son las siguientes:

1. No inscribir el banco de datos en el Registro Nacional de Bases de Datos.
2. Proceder a recoger datos de carácter personal sin proporcionar la debida información conforme con lo establecido en el artículo 8, numeral 2, de esta Ley.
3. Mantener datos de carácter personal inexactos, pese la solicitud de rectificación de los mismos.
4. Mal manejo administrativo del archivo y tratamiento de bases de datos.

**Artículo 25.- Infracciones graves.** Se determinan como infracciones graves las siguientes:

1. Recoger datos en forma engañosa o fraudulenta.
2. Recabar y tratar datos sensibles, sin consentimiento expreso del titular y no guardar la respectiva confidencialidad.

3. Crear bases o bancos de datos, ficheros y archivos con datos sensibles.
4. No atender la solicitud del titular de los datos o de la Autoridad Nacional de Protección de Datos Personales sobre la supresión, rectificación y actualización de los datos personales cuando legalmente proceda.
5. Realizar transferencia temporal o definitiva de datos de carácter personal hacia el extranjero, que hayan sido recogidos u objeto de tratamiento, con destino a organismos gubernamentales, organismos internacionales, ONG, empresas transnacionales públicas y privadas y cualquier otra entidad que no proporcionen ningún nivel de protección, de acuerdo con las normas regionales o internacionales correspondientes.
6. Obstruir las funciones que por esta Ley se le reconoce a la Autoridad Nacional de Protección de Datos.
7. Tratar los datos de carácter personal de un modo que lesione, violente o desconozca los derechos a la intimidad, imagen, identidad y honor, así como cualquier otro derecho de que sean titulares las personas naturales.
8. Obstruir las funciones de vigilancia y control de la Autoridad Nacional de Protección de Datos.
9. Crear bases o bancos de datos, ficheros, archivos, en forma física o digital sobre datos personales sin el cumplimiento de los requisitos establecidos en esta Ley.
10. Iniciar el tratamiento de los datos de carácter personal o usarlos conculcando principios y garantías determinadas en la Constitución y en esta Ley.
11. No guardar la debida confidencialidad sobre los datos de carácter personal incorporados a bases o bancos de datos, ficheros y archivos.
12. Reincidir en cualquier infracción leve.

**Artículo 26.- Sanciones.** Las sanciones que se impondrán a causa del cometimiento de las infracciones señaladas en los artículos precedentes serán:

1. Amonestación por escrito.
2. Multa de uno a diez salarios básicos unificados.
3. Inmovilización de las bases o bancos de datos, ficheros o archivos.
4. Retiro temporal de las bases o bancos de datos, ficheros o archivos.
5. Retiro definitivo de las bases o bancos de datos, ficheros o archivos.

**Artículo 27.- Graduación de las sanciones**. Las sanciones se graduarán según los siguientes lineamientos:

1. Valoración de derechos constitucionales afectados.
2. Volumen de los tratamientos efectuados.
3. Beneficios económicos obtenidos.
4. Grado de intencionalidad.
5. Reincidencia en la comisión de la infracción.
6. Daños y perjuicios causados a titulares o terceras personas.

7. Reconocimiento o aceptación expresa sobre la infracción investigada, antes de la imposición de la sanción.

**Artículo 28.- Procedimiento.** La Autoridad Nacional de Protección de Datos Personales determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación con la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

La máxima autoridad del Ministerio de Telecomunicaciones y Sociedad de la Información será quien resuelva en última y definitiva instancia los recursos que se presenten.

En caso de verificarse la posible existencia de infracción penal, la Autoridad Nacional de Protección de Datos Personales comunicará a las autoridades penales correspondientes para su debida investigación.

## DISPOSICIÓN REFORMATORIA

**ÚNICA.-** Añádase a continuación del numeral 1 del artículo 31 de la Ley del Sistema Nacional de Registro de Datos Públicos el siguiente numeral:

"1.1 Ejercer las funciones como Autoridad Nacional de Protección de Datos Personales conforme a lo dispuesto en la Ley de Protección de Datos Personales."

## DISPOSICIÓN TRANSITORIA

**PRIMERA.-** La Autoridad Nacional de Protección de Datos Personales deberá crear el Registro Nacional de Bases de Datos en el plazo máximo de ciento ochenta días a partir de la publicación de la presente Ley.

**SEGUNDA.-** Para la aplicación de la presente Ley, se dictará el correspondiente Reglamento en el plazo de 90 días.

## DISPOSICIÓN FINAL

La presente Ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Suscrito en Quito, Distrito Metropolitano, a los ... ... .....

REPÚBLICA DEL ECUADOR
ASAMBLEA NACIONAL

**FIRMAS DE RESPALDO AL PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE LOS DERECHOS A LA INTIMIDAD Y PRIVACIDAD SOBRE LOS DATOS PERSONALES**

| NOMBRE | FIRMA |
|---|---|
| Abraham Moya | |
| Hólger Chávez C. | |
| Arger Rivera | |
| Alberto Zambrano | |
| Rene Caza | |
| G. Rivera López | |
| Alberto Arias | |
| Gilberto Guamangate | |
| Diana Moreno | |

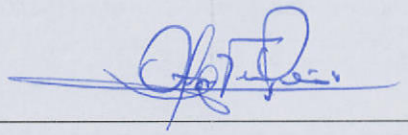
REPÚBLICA DEL ECUADOR
ASAMBLEA NACIONAL

**FIRMAS DE RESPALDO AL PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE LOS DERECHOS A LA INTIMIDAD Y PRIVACIDAD SOBRE LOS DATOS PERSONALES**

| NOMBRE | FIRMA |
|---|---|
| Mauricio Proaño | |
| Oscar Iedesma 2 | |
| Carlos Viteri G. | |
| Marlely Usdonez. | |
| Dora A. Aguirre Hidalgo | |
| Raul Abad Vélez | |
| Rosa Elvira Muñoz | |
| Betty Jerez | |
| Raúl Tobar Núñez | |

REPÚBLICA DEL ECUADOR
ASAMBLEA NACIONAL

# FIRMAS DE RESPALDO AL PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE LOS DERECHOS A LA INTIMIDAD Y PRIVACIDAD SOBRE LOS DATOS PERSONALES

| NOMBRE | FIRMA |
|---|---|
| Octavio Villacres. |  |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |