GRADO EN DERECHO

FACULTAD DE DERECHO SEDE JEREZ DE LA FRA.

TRABAJO DE FIN DE GRADO

JUNIO DE 2022

La Ley Orgánica 7/2021 sobre protección de datos en el ámbito policial

Alumno:

FRANCISCO JAVIER LLERENA CARRASCO

+34 605 61 95 95

franciscojavier.llerenacarrasco@alum.uca.es

Tutor académico:

D. ANTONIO TRONCOSO REIGADA

antonio.troncosoreigada@uca.es

ÍNDICE

RESUMEN

El notable aumento de las amenazas para la seguridad nacional e internacional, algunas ya materializadas en múltiples atentados terroristas por Estados Unidos y Europa, justifican la necesidad de un marco jurídico que tenga por objetivo hacerles frente a través de medidas de prevención, detección, investigación o enjuiciamiento. Para ello, es de vital importancia la cooperación entre las administraciones públicas y la adopción de una normativa armonizada entre los Estados miembros de la Unión que facilite el intercambio de información de carácter personal bajo los principios de coordinación, reciprocidad y eficacia. Desde su nacimiento, la protección de datos personales se ha configurado como un derecho de rango fundamental llamado a garantizar y proteger la esfera privada del individuo y es precisamente la Ley Orgánica 7/2021, de 26 de mayo, traspuesta por Directiva (UE) 2016/680, de 27 de abril, la destinada a asegurar que tales medidas se lleven a cabo conforme a los cauces legales sin lesionar los derechos fundamentales de los afectados por un proceso judicial penal.

Palabras clave: instrucción judicial, administraciones públicas, protección de datos personales, Unión Europea, derecho fundamental.

ABSTRACT

The notably increase of threats to national and international security, some of them already materialized in multiple terrorist attacks along the United States and Europe, justifies the necessity of a legal framework which helps through prevention, detection, investigation, or prosecution measures. For this, it is of vital importance the cooperation between public administrations and the adoption of a harmonized legislation among the State members of the Union to ease the personal information exchange under the principles of coordination, reciprocity, and efficacy. Since its birth, personal data protection has been configured such as a right of fundamental range called to guarantee and protect the private sphere of individuals and it is precisely the Organic Law 7/2021, of 26th May, transposed by the Directive (EU) 2016/680, of 27th April, which is destined to assure that those measures are accomplished within the legal path and without injuring the fundamental rights of the affected by a judicial criminal process.

Key words: judicial investigation, public administrations, personal data protection, European Union, fundamental right.

I. Objetivo y metodología

La presente tesis tiene por objetivo el estudio crítico de la vigente Ley Orgánica 7/2021 desde una perspectiva causal y material, o, en otras palabras, por qué y qué se ha adoptado en relación con la normativa procesal penal aplicable por las autoridades jurisdiccionales y policiales. Para este fin, se analizarán, además de la anterior ley orgánica, tanto la Directiva (UE) 2016/680 del Parlamento y del Consejo, de 27 de abril, motivo principal de la adopción de la ley ya mencionada, como la normativa general de protección de datos –el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018–, las diversas circulares e informes del Supervisor y Comité Europeo de Protección de Datos, la jurisprudencia nacional y del Tribunal de Justicia de la Unión Europea al respecto y los informes de la Agencia Española de Protección de Datos y demás autoridades. Finalmente, en conclusiones se realizará un sucinto análisis de cuál ha sido el impacto de esta la nueva normativa a nivel nacional y en el Espacio Europeo de Seguridad, Libertad y Justicia.

II. Introducción

Desde hace ya varias décadas, toda la Humanidad está viviendo, y sin duda vivirá aún más, una exponencial evolución de la tecnología y la informática. La aparición de una herramienta tan imprescindible como lo es en la actualidad Internet ha significado no tan solo una mejora, sino una revolución en todo tipo de actividades ya sean comerciales, académicas, sociales, de ocio o que revistan cierta relevancia en el ámbito internacional. Es innegable la importancia que tiene y seguirá teniendo Internet y es por ello por lo que el Derecho, como instrumento llamado a regular la vida humana en sociedad, debe intervenir garantizando que aquellas actividades se realicen de la manera más ordenada y pacífica posible garantizando los derechos de los ciudadanos.

En este contexto, el constituyente español, consciente del imparable y arrollador avance de la tecnología, constitucionalizó el entonces llamado derecho a la *libertad informática*[1] en el artículo 18.4 de la Constitución española[2] dentro del derecho al honor, la intimidad personal y familiar y a la propia imagen. Lo cierto

[1] RALLO LOMBARTE, A (dir.), 2019: pág. 26.

[2] Este precepto declara literalmente 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".*

es que este apartado no es más que una manera más de proteger un ámbito de la vida personal privada del individuo –como es su honor y su intimidad tanto personal como familiar en el plano digital– que empezaba a ser violentado a causa de ciertas herramientas informáticas tales como bases de datos y censos electrónicos[3]. Se otorgaba así a este derecho a la libertad informática, que posteriormente derivaría en el actual derecho a la *protección de datos personales*[4], rango de derecho fundamental con los mecanismos de protección propios de este tipo de derechos ex artículo 53 de la Constitución española.

En España, la primera regulación nacional en protección de datos data de 1992[5], normativa que quedó obsoleta debido a la mayor complejidad de los sistemas informáticos. Es por ello por lo que la Unión Europea, consciente de los nuevos retos tecnológicos a los que se debía enfrentar, aprobó el pasado 27 de abril de 2016 un paquete legislativo[6] que modificaría la regulación en materia de protección de datos para hacerla acorde a la nueva realidad. Hay que decir que la opción por parte de las instituciones comunitarias del instrumento normativo

[3] TRONCOSO REIGADA, A (dir.), 2021: pág. 156. Empleando el término *"derecho a la autodeterminación informativa (Recht auf informationelle Selbstbestimmung)"*, fue el Tribunal Federal Alemán –BverfG– el que determinó su definición: *"el derecho de la persona a decidir por sí misma sobre el uso y la divulgación de sus datos personales […]".*

[4] Si bien el Convenio N.º108 del Consejo de Europa fue el primer instrumento internacional en hablar estrictamente del derecho a la protección de datos, a nivel nacional fue la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal la primera en emplear dicho término. El Tribunal Constitucional se encargaría posteriormente de dar una definición concreta de dicho derecho en Sentencia 292/2000 de 30 de noviembre en su fundamento jurídico sexto el cual dispone literalmente que *"el derecho fundamental 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".* Cfr., con la doctrina del BverfG: *"el derecho a la autodeterminación normativa otorga a la persona la facultad –la autoridad– en principio para decidir por sí misma sobre la divulgación y el uso de los datos personales".* TRONCOSO REIGADA, A. (Dir.): 2021, pág. 159.

[5] Posteriormente sería aprobada en España la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal con el objetivo de adaptar el ordenamiento nacional interno a la Directiva 95/46/CE, de 24 de octubre.

[6] Este paquete normativo está compuesto por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 (Reglamento General de Protección de Datos) y la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

de la directiva se debe principalmente al contenido que esta está llamada a regular. Tras el Tratado de Lisboa, que entró en vigor en 2009, la Unión se arrogó competencias en materia penal y policial, que hasta ese momento no eran competencia comunitaria y se desarrollaban en el ámbito de la cooperación entre Estados. Es por ello por lo que la Unión Europea decidió emplear la directiva en lugar del reglamento, pues otorga a los Estados miembros mayor flexibilidad normativa, para regular las cuestiones relativas a la prevención, detección, investigación, enjuiciamiento de infracciones y ejecución de sanciones penales, siempre garantizando una mínima armonización entre los estados miembros y subsanando las deficiencias de la Decisión Marco 2008/977/JAI con el fin de garantizar que el tratamiento de la protección de datos no viole los derechos fundamentales de los afectados.

III. El concepto y ámbito de aplicación de la *"protección de datos personales"* según la Ley Orgánica 7/2021 y la jurisprudencia del Tribunal de Justicia de la Unión Europea

Concepto de "datos personales"

Para comprender el concepto de "protección de datos personales" es necesario, en primer lugar, concretar por separado qué se entiende por "datos personales" definido en el artículo 5.a) de la Ley Orgánica 7/2021[7]. Hemos de interpretar la redacción del precepto desde una perspectiva absolutamente literal pues se incorpora, como señala el artículo a pie de página, todo tipo de información, esto es, ya sea objetiva o subjetiva, cierta o errónea, en relación con el individuo incluyéndose como tal, sin ánimo exhaustivo, el nombre y apellidos, lugar de nacimiento, datos familiares, económicos, sociales o culturales, genéticos, biométricos y los relativos a la salud, parafraseando a ROMEO CASABONA[8].

Un análisis de la jurisprudencia del Tribunal de Justicia de la Unión Europea puede darnos una idea de la amplitud del término. Así, a modo de ejemplo, se consideran datos personales tanto los incluidos en una solicitud de residencia o

[7] A tales efectos el artículo 5 de Ley Orgánica 7/2021 expone un catálogo de definiciones, pero nos limitaremos a analizar el apartado a) el cual dispone que "*se entenderá por datos personales toda información sobre una persona física identificada o identificable".* Lo cierto es que esta definición de dato personal es exactamente la misma que la recogida tanto en el Reglamento (UE) 2016/679 como en la Directiva (UE) 2016/680.

[8] Vid. ROMEO CASABONA, en TRONCOSO REIGADA, A (dir.), 2021: pág. 574

los relativos a un trabajador en un registro de trabajo como las direcciones IP (vid. respectivamente la STJUE de 17 de julio de 2014, asunto YS, C-141/12; la STJUE de 30 de mayo de 2013, asunto Worten, C-342/12; y las SSTJUE de 19 de octubre de 2016, asunto Breyer, C-582/14 y de 24 de noviembre de 2011, asunto Scarlet Extended, C-70/10). Un importante, y cuanto menos curioso, matiz por mencionar es este último ejemplo: la consideración por parte del Tribunal de Justicia de la Unión Europea de la IP –*Internet Protocol*[9]– como dato personal.

La dirección IP de cualquier dispositivo conectado a la red no permite identificar *per se* directamente a la persona que está empleando tal dispositivo, en cambio sí que permite identificarla. En otras palabras, la IP no es un dato que determine la identidad de una persona, pero sí la hace potencialmente identificable. Por poner un ejemplo, conocer únicamente la IP de un ordenador portátil no nos permite conocer la identidad de la persona que utiliza ese portátil, pero sí es una información o dato que, sumado a otros, permite individualizar a aquella persona[10]. Es precisamente este argumento el que emplea el Tribunal de Justicia de la Unión Europea para aceptar a la IP como dato personal y por ende, dentro del ámbito de aplicación de la Ley Orgánica 7/2021 objeto de estudio[11]. En estos

[9] Según el Diccionario panhispánico del español jurídico una IP es una "*información numérica de un elemento conectado a una red que utiliza el protocolo TCP/IP"* el cual, a su vez, es un sistema que facilita la conexión y el intercambio de datos entre dos usuarios. Hay que hacer una distinción entre las IP estáticas y las dinámicas: las primeras se caracterizan por ser invariables y permitir la identificación permanente del dispositivo y las segundas son aquellas que se asignan de forma provisional para cada conexión a la red modificándose en conexiones posteriores. Ambas son consideradas datos personales.

[10] Nótese la diferencia entre "persona identificada" y "persona identificable". La primera es una que conocemos, mientras que la segunda es una susceptible de conocer. El considerando 21 de la Directiva (UE) 2016/680 indica que *"para determinar si una persona física es identificable deben tenerse en cuenta todos los medios con respecto a los cuales existe una probabilidad razonable de que puedan ser utilizados por el responsable del tratamiento o por cualquier otra persona para la identificación directa o indirecta de dicha persona física".*

[11] La mencionada STJUE de 19 de octubre de 2016, asunto Breyer, C-582/14 concluye que "*una dirección IP dinámica registrada por un proveedor de servicios de medios en línea con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público constituye respecto a dicho proveedor un dato personal cuando éste disponga de medios legales que le permitan identificar a la persona interesada gracias a la información adicional de que dispone el proveedor de acceso a Internet de dicha persona"*. En otras palabras, la dirección IP es un dato personal por tratarse de una información susceptible de identificar a una persona física, cfr. con el artículo 5.a) de la Ley Orgánica 7/2021 en la medida en que esa persona debe de estar identificada o ser identificable.

mismos términos se expresaba también el Informe 327/2003 de la Agencia Española de Protección de Datos[12].

Ahora bien, no todos los datos personales son del mismo tipo o requieren el mismo grado de protección por el contenido informativo que contienen. Existen así las llamadas *"categorías especiales de datos personales"*[13] entre las que se encontrarían los datos relativos al origen étnico o racial, datos genéticos, o los relativos a la salud o a la vida u orientación sexual del interesado, entre otras. En la Ley Orgánica 7/2021 se dice que el tratamiento de estas categorías esenciales, que habrá de tener el requisito de identificar de manera unívoca a una persona, deberá respetar los siguientes requisitos de carácter acumulativo:

A) Cuando el tratamiento sea estrictamente necesario, y,

B) Cuando lo prevea una norma con rango de ley o por el Derecho comunitario; cuando resulte necesario para la proteger la vida del afectado u otra persona física; cuando se refiera a datos que el interesado haya hecho públicos.

En el apartado segundo del artículo 13 de la Ley Orgánica 7/2021 se hace una previsión excepcional en relación con los datos biométricos, que no genéticos[14], cuando, de nuevo, se persiga el fin que prevé el artículo 1, de manera que la autoridad podrá tratar aquellos datos dirigidos a identificar de forma unívoca a la persona física.

Ámbito de aplicación material u objetivo

Antes de todo, hay que partir de la idea de que esta regulación se adopta como adición a la regulación de protección de datos personales general recogida en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. Es por esto por lo que el objeto de aplicación de la Ley Orgánica 7/2021 tendrá por excluida todas las cuestiones que sean objeto de aplicación por las dos normas anteriormente mencionadas. Además, se tienen por excluidas otras materias a

[12] "*Desde esta Agencia de Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos."*

[13] Vid el artículo 13 de la Ley Orgánica 7/2021 y 10 de la Directiva (UE) 2016/680.

[14] Vid. la diferencia entre ambos conceptos en el artículo 5 de la Ley Orgánica 7/2021.

las que hace referencia el mismo precepto en apartados posteriores tales como los realizados por la Administración General del Estado en relación con la política exterior y la seguridad común; los tratamientos que afecten a actividades no comprendidas por el Derecho comunitario; aquellos relativos a la Defensa Nacional; así como las acciones civiles y administrativas vinculadas a procesos penales que no tengan como objetivo los fines de los artículos 1 y 2 de la Ley[15].

A partir de este breve inciso, el apartado 1 del artículo 2 de la Ley Orgánica 7/2021 dice que *"será de aplicación 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, realizado por las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública."* Este ámbito de aplicación material se limita a lo que AMÉRIGO ALONSO denomina *"actividades preventivas y punitivas de delitos y de ejecución de sanciones penales […] orientadas a garantizar la eficacia de la cooperación judicial y policial"*[16].

No hay que confundir, pues no son los mismos, los fines del artículo 1 y 2 de la Ley Orgánica 7/2021 con los del artículo 10 del Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, los cuales se refieren al tratamiento de los datos personales relativos a condenas e infracciones *penales.* Siguiendo la redacción del mismo reglamento, el precepto se refiere *"al tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas […], sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas"*. Véase que tanto el Reglamento (UE) 2016/679 como la Ley Orgánica 3/2018 son de aplicación cuando existe una condena penal firme[17], mientras que la Ley Orgánica 7/2021 es de aplicación

[15] A esto se refiere el artículo 2.3 de la Ley Orgánica 7/2021.
[16] Vid. AMÉRIGO ALONSO, en RALLO LOMBARTE, A (dir.), 2019: pág. 98.
[17] De hecho, el artículo 10 de la Ley Orgánica 3/2018 dice literalmente que *"el tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y*

previa, esto es según los artículos 1 y 2, a los tratamientos relativos a la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. De hecho, la autora GOMEZ NAVAJAS distingue dos tipos de datos de naturaleza penal a los que les son de aplicación o bien el reglamento o bien la directiva. Estos datos son los relativos a infracciones y condenas penales o medidas de seguridad conexas que entran dentro del campo de aplicación del Reglamento (UE) 2016/679; y los relativos a la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluyendo la protección frente a amenazas a la seguridad pública y su prevención que entran dentro de la aplicación de la Directiva (UE) 2016/680[18].

El artículo 2 de la Ley Orgánica 7/2021 habla de "tratamiento de datos". El artículo 5.b) de la Ley Orgánica 7/2021 da una definición aclaratoria al respecto[19], al tenor de la cual concluimos que se trata de un concepto de tal amplitud que prácticamente cualquier operación que se realice en relación con datos personales tendrá la consideración de tratamiento. Parece coherente pensar que el motivo que lleva al legislador a admitir un concepto lo más amplio posible de "tratamiento" y de "datos" es el de ampliar al máximo el alcance de la normativa que tiene como fin supremo la protección de los datos privados del particular. Dicho esto y, para visualizar de una manera más aclaratoria la amplitud del término, se podría traer a colación la STJUE de 13 de mayo de 2014, asunto Google Spain, C-131-12, en la que se considera tratamiento de datos el hecho de que un motor de búsqueda online, en este caso Google, emplee información publicada por terceras personas con el fin de indexarla, almacenarla y ponerla a disposición de los usuarios de internet siguiendo un orden de preferencia determinado, todo ello de manera automática.

medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales […]".

[18] Vid. GÓMEZ NAVAJAS, en TRONCOSO REIGADA, A. (dir.): 2021, págs. 1281-1314.

[19] *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.*

Por todo lo dicho, podríamos concluir de manera resumida que el objetivo material de esta normativa es el de conseguir una regulación lo suficientemente eficiente y armonizada para que ese tratamiento de datos en relación con los fines de prevención, detección, investigación judicial, etc., se realice sin lesionar los derechos de los afectados, idea respecto de la cual incide el Considerando 7 de la Directiva (UE) 2016/680[20].

Ámbito de aplicación subjetivo

Nos compete ahora analizar el campo subjetivo de la Ley Orgánica. No cabe duda de que se trata de una normativa que se aplica a las personas, en general, aunque si bien exclusivamente a las físicas, en particular. El de nuevo mencionado artículo 5.a) de la Ley Orgánica 7/2021 identifica a la persona física identificada o identificable como "el interesado"[21] y verdaderamente es este el individuo al que en todo momento se refiere el articulado de dicha ley, es decir, su verdadero ámbito de aplicación subjetivo. No existe mayor dificultad en definir persona física[22] más allá del matiz identificada o identificable al que ya hemos hecho referencia anteriormente, por lo que vista la vertiente de la aplicación subjetiva positiva, procedemos a ver la vertiente negativa, o sea, a quienes no se les aplica la normativa de protección de datos.

La Ley Orgánica 7/2021 excluye a las personas jurídicas del artículo 35 del Código Civil y con ellas también a los entes carentes de personalidad jurídica –por ejemplo herencias yacentes…–, además de las personas fallecidas; exclusión que también realiza el Reglamento (UE) 2016/679 como se desprende de sus Considerandos 14 y 27. La razón por la que las personas jurídicas quedan excluidas es simple, pues la normativa únicamente hace referencia a persona física y en ningún momento a "persona jurídica" o a "persona" sin más. Si bien en algunas legislaciones europeas se incorporaron en su momento ciertas

[20] *"[…] A tal efecto, el nivel de protección de los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública, debe ser equivalente en todos los Estados miembros […]".*

[21] TRONCOSO REIGADA, A. (dir.), 2021: pág. 575. ROMEO CASABONA define al interesado como *"el titular de los derechos que sobre los propios datos se reconocen en el Reglamento General de Protección de Datos".*

[22] Un ser humano que, en virtud del artículo 29 y 30 del Código Civil, se ha desprendido plenamente del claustro materno.

disposiciones complementarias a la Directiva 95/46/CE aplicables a las personas jurídicas[23], en el ordenamiento español se ha optado por seguir la corriente comunitaria de excluir a las personas jurídicas, y con ellas a los entes carentes de personalidad.

Por otro lado, la Ley Orgánica 7/2021 excluye igualmente de su ámbito de aplicación a las personas fallecidas en el apartado 4 del artículo 2[24]. La justificación también resulta sencilla pues, sobrevenida la muerte, se produce la extinción de la personalidad jurídica ex artículo 32 del Código Civil. Ahora bien, la persona fallecida deja tras de sí una ingente cantidad de datos respecto de los cuales, si bien ya no es titular, sí que despliegan ciertos efectos que recaen a modo de derechos sobre las personas vinculadas a aquella como se desprende del artículo 3 de la misma Ley Orgánica[25]. Se trata básicamente de un derecho de acceso, rectificación o supresión de los datos del fallecido que podrán ejercer los familiares y herederos del fallecido o, en caso de menores, el propio Ministerio Fiscal frente al responsable o encargado del tratamiento. El contenido de estos derechos será analizado más adelante.

Aunque la Ley Orgánica 7/2021 no excluye en su articulado a los no nacidos, la doctrina sí lo hace puesto que el no nacido aún no es persona al no haberse cumplido lo dispuesto en los anteriores artículos 29 y 30 del Código Civil, aunque con ciertas matizaciones como afirma ROMEO CASABONA[26] en los siguientes términos: *"los datos que prevalentemente son susceptibles de plantear su protección en relación con el no nacido, a pesar de no haber adquirido todavía la condición de persona son los relativos a la salud y filiación biológica."*

[23] Vid. el caso de Austria o Italia. Sobre esta cuestión incide HERRÁN ORTIZ, A. 1998: pág. 233 y ss.

[24] *Esta Ley Orgánica no se aplicará a los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo siguiente.*

[25] DÍAZ ALABART, S., 2020: pág. 77 y ss. Si bien esta ley no hace referencia al derecho al testamento digital, como por el contrario sí hace la Ley Orgánica 3/2018 en el artículo 96, al mencionar la figura del heredero podemos pensar que aquel derecho se aplicaría de forma supletoria a esta normativa especial. DÍAZ ALABART destaca las dificultades de tramitación parlamentaria a la hora de adaptar la normativa española a la comunitaria debido principalmente al matiz que realiza el artículo 96.4 en relación con los derechos civiles forales. Dificultades que se materializó con la aprobación de *Llei 10/2017, de 24 de juny, de les voluntats digitals i de modificación dels llibres segon i quart del Codi civil de Catalunya,* declarada parcialmente inconstitucional mediante STC 7/2019, de 17 de enero.

[26] Vid. ROMEO CASABONA, en TRONCOSO REIGADA, A. (dir.) 2021: pág. 581 y 582. Este autor afirma que los datos relativos a los no nacidos entrarían dentro de la normativa de protección de datos personales por calificarlos como categorías especiales de datos personales ex artículo 9.1 del Reglamento (UE) 2016/679.

Siguiendo al mismo autor, los datos del no nacido son informaciones que pueden llegar a manos de a terceras personas y debe ser el objetivo de la ley la protección *a futuro* de sus datos personales hasta que nazca, momento en que adquirirá la personalidad y con ella la condición de titular o interesado.

Al igual que existen las categorías especiales de datos, la Ley Orgánica 7/2021 también distingue categorías de interesados en el artículo 9[27]. Así, el responsable del tratamiento distinguirá entre: aquellas personas respecto de que existan motivos fundados para presumir que hayan cometido, puedan cometer o colaborar en un delito; personas condenadas; víctimas o afectados por algún delito; terceros involucrados en la comisión de un delito. Por supuesto esta previsión legal no podrá en ningún caso lesionar el derecho fundamental a la presunción de inocencia que establece el artículo 24 de la Constitución.

Finalmente, aparte de hacer referencia a las personas a quienes se les aplica la Ley Orgánica 7/2021, hemos de hacer referencia a aquellas responsables de aplicarla, o en otras palabras, las personas competentes para el tratamiento de los datos personales a que se refiere el artículo 1. Estas son, de conformidad con el artículo 4 de las autoridades competentes de la Ley, las Fuerzas y Cuerpos de Seguridad del Estado –en concreto los cuerpos tanto nacional como autonómicos de policía y la Guardia Civil–, las administraciones penitenciarias, la Dirección Adjunta de Vigilancia Aduanera de la Administración Estatal de la Agencia Tributaria, el Servicio Ejecutivo de la Comisión de Prevención del Blanqueo de Capitales e Infracciones Monetarias, la Comisión de Vigilancia de Actividades de Financiación del Terrorismo y, por supuestos, las autoridades judiciales del orden jurisdiccional penal y el Ministerio Fiscal.

Acabando con este epígrafe, hemos de incidir en la idea de que necesariamente deben acumularse los presupuestos de finalidad (ámbito de aplicación objetivo) y autoridad (ámbito de aplicación subjetivo) para que la Ley Orgánica 7/2021 sea de aplicación[28]. Esto quiere decir por ejemplo que el tratamiento de los datos personales que realice un policía nacional en el momento de expedir el DNI o el visado a una persona, o cualquier otro tipo de trámite de carácter administrativo,

[27] Por mandato del Considerando 31 de la Directiva (UE) 2016/680.

[28] ARANGÜENA FANEGO, C. y DE HOYOS SANCHO, B. (dir.), 2018: pág. 390. Cfr. con el artículo 11 de la Ley Orgánica 7/2021 en la medida en que deben de cumplirse los fines del artículo 1 y se realice por autoridad competente.

no entraría dentro del campo de aplicación de la normativa a la que aquí hacemos referencia, puesto que, en este caso, únicamente se daría el presupuesto subjetivo, y no objetivo, al igual que tampoco la finalidad de la Ley Orgánica 7/2021.

IV. Principios generales de la Ley Orgánica 7/2021

Los principios generales de actuación de la Ley Orgánica 7/2021 se detallan a modo de catálogo en el artículo 6, dentro del Capítulo II que lleva por rúbrica "los principios, licitud del tratamiento y videovigilancia", en relación con el artículo 4 de la Directiva (UE) 2016/680. Estos son los siguientes: el principio de licitud y lealtad, el principio de limitación de la finalidad, el principio de minimización de datos, el principio de exactitud, el principio de limitación del plazo de conservación, el principio de integridad y confidencialidad y por último el principio de responsabilidad proactiva. Lo cierto es que esta normativa especial, objeto de estudio en el presente trabajo, no desarrolla estos principios rectores de actuación por lo que se ha tenido que acudir a la normativa general, esta es el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, para desarrollar la definición y función de cada uno de ellos[29].

Curiosa es la supresión del principio de transparencia que realiza tanto la Directiva (UE) 2016/680 como la Ley Orgánica 7/2021 en relación con la figura del interesado, principio que sí que se encuentra previsto en el Reglamento (UE) 2016/679. Esta supresión, según RODRÍGUEZ-MEDEL NIETO, se debe como es lógico a los propios fines de la Directiva (UE) 2016/680 y la Ley Orgánica 7/2021, pues la consecución de las actuaciones de prevención, investigación y detección de infracciones penales podrían peligrar si el tratamiento de datos personales hubiese de ser transparente en relación con el interesado[30]. En otras palabras, si el investigado en un proceso judicial penal conoce del tratamiento de sus datos personales, este puede llevar a cometer una serie de actuaciones destinadas a dificultar o impedir la instrucción de la causa. Dicha esta salvedad

[29] TRONCOSO REIGADA, A. (dir.): 2021, pág. 850. TRONCOSO REIGADA, en relación con el considerando 10 del Reglamento (UE) 2016/679, dice que *"la incorporación de unos principios relativos al tratamiento […] es un elemento esencial […] para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión".*

[30] Vid. RODRÍGUEZ MEDEL-NIETO, en ARANGÜENA FANEGO, C. y DE HOYOS SANCHO, B. (dir.), 2018: pág. 394.

y partiendo de la idea de que el resto de los principios rectores que inspiran la aplicación de la Ley Orgánica 7/2021 son los mismos que los recogidos en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018, a continuación se analizarán uno por uno los distintos principios.

Principio de licitud y lealtad

Dice el artículo 6.1.a) de la Ley Orgánica 7/2021 que *"los datos personales serán tratados de manera lícita y leal"* y, relacionando este precepto con el artículo 11 del mismo cuerpo normativo, se entenderá que el tratamiento es lícito "*en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice con una autoridad competente en ejercicio de sus funciones".*[31]

Al no exigirse el consentimiento del afectado para el tratamiento de sus datos personales de forma que se respete el principio de licitud y lealtad, se ha de dar lo que PUENTE ESCOBAR denomina *"interés legítimo prevalente*[32]*"* y es de hecho el Dictamen 6/2014 del Grupo de Trabajo del Artículo 29[33] de la Directiva 95/46/CE el que viene a concretar lo que hemos de entender por ello. Así, "*el interés debe ser lícito (es decir, ser conforme a la legislación nacional y de la Unión Europea), estar articulado con la claridad suficiente para permitir que la prueba de sopesamiento se realice en contraposición a los intereses y los derechos fundamentales del interesado (es decir, ser suficientemente concreto) y representar un interés real y actual (es decir, no especulativo)*[34]*".*

Por lo que respecta al principio de lealtad LÓPEZ ÁLVAREZ lo explica de la siguiente manera, en relación con la Resolución R/03360/2015 de la Agencia Española de Protección de Datos, *"el tratamiento de datos no debe ser solo legal, sino también leal, lo que significa que la información que se presta al titular de los datos sea adecuada al afectado o interesado, para que conozca el alcance real del consentimiento que presta o, en caso de no precisarse –como es el caso*

[31] Cfr. con el artículo 6 del Reglamento (UE) 2016/679 en la medida en que ni la Directiva (UE) 2016/680 ni la Ley Orgánica 7/2021 exige el consentimiento del afectado sino únicamente en la necesidad del tratamiento para la consecución de los fines de la propia directiva.
[32] PUENTE ESCOBAR, A. (dir.), 2019: pág. 126.
[33] El Grupo de Trabajo del Artículo 29 es el predecesor del actual Comité Europeo de Protección de Datos, o EDPB, por sus siglas en inglés.
[34] Dictamen 6/2014 de 9 de abril del Grupo de Trabajo del Artículo 29 (Documento WP 217), pág. 65.

de la Ley Orgánica 7/2021– los fines de la recogida y el modo de ejercitar los derechos[35]".

Desde mi punto de vista, el principio de lealtad se debería ver desde el punto de vista de que los responsables del tratamiento no van a emplear los datos para otros fines distintos o contrarios a los que originaron el inicio del tratamiento de manera que se pudiese lesionar los derechos fundamentales de los afectados por un tratamiento desleal, perjudicial, discriminatorio o engañoso[36].

Principio de limitación de la finalidad

Dice el artículo 6.1.b) de la Ley Orgánica 7/2021 que *"los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con otros fines"[37]*. No parece haber mayor dificultad en la comprensión de este principio rector, pues básicamente se aporta la idea de que el tratamiento de los datos personales del afectado no podrá destinarse a otros fines distintos de los que originaron el inicio del tratamiento ni por supuesto destinarse a fines contradictorios a los de la ley.

De nuevo el Grupo de Trabajo del Artículo 29 analizó el alcance de este principio en Dictamen 3/2013 de 2 de abril (Documento WP 203). PUENTE ESCOBAR resume la idea del dictamen con las siguientes palabras: *"viene a considerar que el tratamiento de los datos para fines que no coincidan con los que justificaron su recogida exigirá un doble examen: el de compatibilidad del fin y el de concurrencia de una base jurídica de dicho tratamiento"[38].*

---

[35] LÓPEZ ÁLVAREZ, L.F., 2017: pág. 31.

[36] En este sentido, se expresan las Guidelines 4/2019 on Article 25 Data Protection by Design and by Default adopted on 13 November, pág.16: *"personal data shall not be processed in a way that is detrimental, discriminatory, unexpected or misleading to the data subject".* Seguidamente, el documento da una serie de elementos que debe acompañar al principio de lealtad.

[37] Cfr. con el apartado dos del artículo 6: *"los datos personales recogidos por las autoridades competentes no serán tratados para otros fines distintos de los establecidos en el artículo 1, salvo que dicho tratamiento esté autorizado por el Derecho de la UE o por la legislación española […]*".

[38] PUENTE ESCOBAR, A. (dir.), 2019: pág. 154. El autor simplemente incide en la idea de que el Dictamen exige necesariamente la concurrencia de los dos requisitos mencionados de forma que sean cumulativos para poder considerar que existe el principio de limitación de la finalidad. En otras palabras, los límites a la finalidad del tratamiento de los datos de la Ley Orgánica 7/2021 se discierne por un lado cuando la finalidad del tratamiento es la misma que la finalidad mediante la que se obtienen los datos y por otro lado cuando existe una base jurídica sólida o, mejor dicho, justificada para ello. Cfr. con el Considerando 50 del Reglamento (UE) 2016/679 que afirma 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. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales […]".*

Este principio en cuestión está interconectado de alguna manera con el principio de licitud y lealtad, pues si se estuviese destinando el tratamiento a fines distintos de aquellos que justificaron el inicio o de los permitidos por la normativa, el responsable estaría incurriendo en una lesión de la licitud y lealtad del tratamiento extralimitándose en la finalidad que lo originó.

Principio de minimización de datos

Conforme dispone el artículo 6.1.c) de la Ley Orgánica 7/2021, los datos personales serán *"adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados"*. Vista esta afirmación, nos centraremos en el punto de que los datos deben ser *no excesivos*, a sensu contrario deben ser reducidos, o sea los mínimos posibles de ahí el nombre del principio. Esto es así por el tipo de datos personales que en virtud de la Ley Orgánica 7/2021 el responsable del tratamiento está llamado a tratar, siendo susceptible ese tratamiento de violentar los Derechos Fundamentales de los afectados –el primero el derecho a la presunción de inocencia–.

Así, la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, enlaza con lo que la jurisprudencia constitucional ha denominado principios de idoneidad, necesidad y proporcionalidad.[39] Sucintamente, los datos deben ser los menos posibles, en cantidad, e invasores, en cualidad, para alcanzar el fin que se pretende mediante el tratamiento[40].

A pesar de intentar definir de manera aislada el principio de minimización, lo cierto es que este no puede entenderse si no es de la mano del siguiente principio rector que se analiza a continuación.

[39] Vid. a estos efectos las STC 207/1996, de 16 de diciembre, la cual afirma en su Fundamento Jurídico 4.E) que "*para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)»".*

[40] Vid en este sentido el Informe 0065/2015 de la Agencia Española de Protección de Datos.

Principio de limitación del plazo de conservación

Dice el artículo 6.1.e) de la Ley Orgánica 7/2021 que los datos personales serán *"conservados de forma que permitan identificar al interesado durante un período no superior al necesario para los fines para los que son tratados"*. La Ley no aporta ningún plazo más allá del general de veinte años ex artículo 8, siempre y cuando no concurran otros factores que, a modo de excepción, ampliarían aún más el plazo de manera indefinida[41]. La normativa únicamente se limita a establecer que la conservación de los datos personales tendrá lugar únicamente *"durante el tiempo necesario"* y que será el responsable del tratamiento quien, cada tres años como máximo, deberá revisar la necesidad de conservarlos, limitarlos o suprimirlos[42], previo lo cual tendrá la obligación del bloqueo de los datos[43].

De hecho, el Comité Europeo de Protección de Datos entiende este principio, en concreto las medidas y garantías que este reconoce, como un complemento a los derechos y libertades que la normativa de protección de datos reconoce, principalmente al derecho de supresión (la doctrina habla del derecho "al olvido") y de oposición[44].

Es decir, la conservación de los datos no puede prolongarse indefinidamente en el tiempo de forma que, si el tratamiento llega a ser irrelevante o transcurrido el plazo general de veinte años, el responsable tiene la obligación de bloqueo vista.

Principio de exactitud

Dispone el artículo 6.1.d) de la Ley Orgánica 7/2021 que los datos personales serán *"exactos y, si fuera necesario, actualizados. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen, sin dilación indebida, los datos personales que sean inexactos con respecto a los fines para los que*

[41] Por ejemplo, en caso de delitos no prescritos o investigaciones abiertas, reincidencia, necesidad de protección de las víctimas u otras circunstancias debidamente motivadas.
[42] Vid la dicción del artículo 8 de la Ley Orgánica 7/2021.
[43] El bloqueo de los datos, a diferencia de la supresión, rectificación o limitación del tratamiento que son derechos de los interesados, es una obligación o deber del responsable de manera que se impida el tratamiento con el objetivo de la futura destrucción de los datos. Vid. el artículo 32 de la Ley Orgánica 3/2018.
[44] Vid. Las Guidelines 4/2019 on Article 25 Data Protection by Design and by Default adopted on 20th October, pág. 25: *"Measures and safeguards that implement the principle of storage limitation shall complement the rights and freedoms of the data subjects, specifically, the right to erasure and the right to object".*

son tratados[45]*".* Podríamos relacionar este artículo con el 10 de la misma ley, el cual hace referencia a la obligación del responsable del tratamiento de verificar la calidad de los datos con los que trabaja[46].

Como bien justifica en sus Guidelines 4/2019 de 19 de noviembre, el Comité Europeo de Protección de Datos, el tratamiento de datos personales inexactos o equívocos puede suponer un claro riesgo para los derechos y libertades de los interesados, quienes se verían afectados sin motivo aparente llegándose en el peor supuesto posible, a vulnerar su derecho constitucional a la presunción de inocencia recogido en el artículo 24 de la Constitución española[47].

Principio de integridad y confidencialidad

El artículo 6.1.f) de la Ley Orgánica 7/2021 declara que los datos personales serán "*tratados de manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no automatizado o ilícito y contra su pérdida, destrucción o daño accidental. Para ello, se utilizarán las medidas técnicas u organizativas adecuadas".*

El precepto incide en la idea de la seguridad para garantizar tanto la integridad como la confidencialidad de los datos. Por un lado, MESSÍA DE LA CERDA BALLESTEROS indica que los términos integridad y confidencialidad hacen referencia *"a la necesidad de arbitrar medidas que impidan la manipulación y posible alteración del contenido de la información y a la necesidad de evitar su puesta en conocimiento de terceros*[48]*".*

[45] Desde mi punto de vista, la ley comete una redundancia innecesaria al decir que los datos deberán ser exactos y actualizados. Máxime cuando se dice *si fuera necesario* pareciendo relegar la actualidad de la información o del dato en un segundo plano, únicamente cuando fuese posible. Si el dato no es exacto jamás puede estar actualizado pues no es atribuible a ninguna persona, y en sentido contrario, si no está actualizado es que no es exacto pues habrá sido atribuible o no en el pasado a una persona, pero no en la actualidad.

[46] Esta disposición recoge la obligación del responsable del tratamiento de distinguir aquellos datos que se basen en hechos, y que por ende sean ciertos, de aquellos basados en apreciaciones personales. Por supuesto, se establecen otra serie de obligaciones tales como el de no transmitir información inexacta o desactualizada o, en caso de haberlo hecho, comunicarlo al destinatario y rectificar lo antes posible. Como se ve el artículo 10 no es más que una extensión aclaratoria del principio de exactitud, e incluso del principio de lealtad.

[47] Vid el artículo 9 de la Ley Orgánica 7/2021 de las categorías de interesados por parte del responsable. Un uso incorrecto o desactualizado de los datos podría derrumbar la presunción de un individuo por considerarlo sospechoso de la comisión de un delito.

[48] Vid, MESSÍA DE LA CERDA BALLESTEROS, en TRONCOSO REIGADA, A. (dir.): 2021, pág. 913.

A lo anterior responde el Comité Europeo de Protección de Datos en las *Guidelines* que se han mencionado, las cuales afirman que son necesarias una serie de actuaciones para impedir o gestionar los incidentes de vulneración de datos, para garantizar la ejecución del tratamiento acorde con los principios o facilitar los derechos de los interesados. De nuevo según el Comité, esto se podría realizar mediante el *Information Security Management System (ISMS)* que es un medio operativo para gestionar políticas y procedimientos de seguridad de la información de forma que se garantice la accesibilidad, confidencialidad, integridad y disponibilidad de los datos.

Principio de responsabilidad proactiva[49]

Este último principio viene recogido en el apartado 5 del artículo 6 de la Ley Orgánica 7/2021 el cual dispone que *"el responsable del tratamiento deberá garantizar y estar en condiciones de demostrar el cumplimiento de lo establecido en este artículo"*. De aquí, únicamente extraemos la idea de que el responsable[50] es la figura que tiene el deber de, por ejemplo, como hemos visto y sin ánimo exhaustivo, –pues existen otras obligaciones– controlar los plazos de conservación y revisión ex artículo 8; de distinguir entre las distintas categorías de interesados *ex* artículo 9; o de verificar la calidad de los datos personales *ex* artículo 10.

Es decir, este principio de responsabilidad proactiva únicamente reconoce la obligación del responsable del tratamiento de garantizar el cumplimiento o respeto de todos los principios rectores anteriores y a responder en caso de incumplimiento de alguno de ellos.

[49] ARANGÜENA FANEGO, C y DE HOYOS SANCHO, M. (dir.), 2018: pág. 395. En el capítulo en que escribe la autora RODRÍGUEZ-MEDEL NIETO, esta considera la obligación del responsable del tratamiento como un principio rector. Podríamos entender que el principio rector de responsabilidad proactiva es una suerte de pilar sin el cual todo el sistema de principios se desmoronaría en tanto en cuanto el responsable es el garante del respeto del resto de principios.

[50] Según el artículo 5.g) de la Ley Orgánica 7/2021 el responsable del tratamiento es "*la autoridad competente que sola o conjuntamente con otras, determina los fines y medios del tratamiento de datos personales".* Continúa el precepto añadiendo que *"en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la UE o por la legislación española, dichas normas podrán designar al responsable del tratamiento, o bien los criterios para su nombramiento".* Por poner un ejemplo, en una investigación judicial de carácter penal, sería el juez instructor quien actúa en calidad de responsable del tratamiento, poniendo esta disposición legal en relación con el artículo 4 de la misma Ley.

Para mayor abundamiento, las *Guidelines* 4/2019, de 13 de noviembre, del Comité Europeo de Protección de Datos aporta una serie de supuestos prácticos en relación con cada uno de los distintos principios rectores a que se ha hecho referencia en el análisis anterior, a modo meramente ilustrativo.

V. Derechos de las personas. Especial consideración del Derecho al Olvido en la Ley Orgánica 7/2021. Ejercicio y límites a los derechos.

En el Capítulo III de la Ley Orgánica 7/2021 se recogen los derechos de las personas en materia de protección de datos. Tradicionalmente la doctrina ha venido denominando al conjunto de derechos que asisten a los interesados en materia de protección de datos como *"los derechos ARCO".* La palabra ARCO no es más que un acrónimo con las primeras letras de los derechos de Acceso, Rectificación, Cancelación y Oposición. A este conjunto de derechos debe añadirse el derecho del *"sospechoso o causado a ser informado de que sus datos personales son objeto de tratamiento"* como añade GUTIÉRREZ ZARZA. Siguiendo a esta misma autora, en el seno de la Unión Europea, aquellos que están siendo investigados por una causa penal ya tenían el derecho a ser informados del motivo por el que estaban siendo investigados y el acceso al expediente judicial sin necesidad de reconocerles el equivalente a estos derechos en materia de protección de datos personales, además por otro lado, el reconocimiento de estos principios puede llegar a colisionar con el principio acusatorio y las normas relativas a la carga de la prueba, pues *"el derecho procesal penal tiene sus propios cauces para que el sospechoso intente desvirtuar los hechos que se le imputan y que le resultan desfavorables"*[51].

De hecho, la propia Directiva (UE) 2016/680 permite la no aplicación de los derechos ARCO cuando estos colisionen con la normativa procesal penal nacional[52]. En resumen, a pesar de que la Directiva (UE) 2016/680 reconoce los derechos que a continuación se analizan, la normativa procesal penal prevalece.

[51] ARAGÜENA FANEGO, C y DE HOYOS SANCHO, M. (dir.), 2018: pág.445 y 446.

[52] Vid el Considerando 107 el cual afirma que *"la presente Directiva no debe impedir que los Estados miembros regulen el ejercicio de los derechos de los interesados en materia de información, acceso a los datos personales, rectificación o supresión de estos y limitación de su tratamiento en el marco de un proceso penal, y las posibles restricciones de tales derechos, mediante el Derecho procesal penal nacional".*

Así se desprende de la dicción de varios preceptos de la Ley Orgánica 7/2021, véase como ejemplo el artículo 26 de los derechos de los interesados como consecuencia de investigaciones y procesos penales[53] en relación con el artículo 2.2 y las disposiciones finales primera a octava de la Ley por las que se modifican algunos artículos de contenido procesal de la Ley Orgánica 6/1985 del Poder Judicial y la Ley 50/1981 del Estatuto Orgánico del Ministerio Fiscal, entre otras[54].

La Ley Orgánica 7/2021, en los artículos 20, 21 y 25, aporta unos elementos básicos en lo que respecta al ejercicio de los derechos antes de entrar en cada derecho en concreto, artículos 22 a 24. Conviene pararnos a mirar en primer lugar las disposiciones 20 y 21, del derecho a la información que debe ponerse a disposición del interesado, y finalmente la 25.

Los dos primeros preceptos van dirigidos a la figura del responsable del tratamiento. Sucintamente, el responsable deberá poner a disposición del interesado de una manera completamente inteligible por cualquier individuo la información siguiente: quién es el responsable del tratamiento; en su caso, los datos de contacto del delegado de protección de datos; los fines del tratamiento a los que se destinen los datos personales; el derecho de presentar reclamación ante la autoridad de protección de datos competente; y la posibilidad de ejercer los derechos del artículo 22 a 24. Por supuesto, la información se suministrará gratuitamente y debida y legalmente motivada mediante cualquier medio adecuado, incluidos los electrónicos, indicando el plazo durante el cual se conservarán los datos y las categorías de destinatarios, entre otras cuestiones[55].

---

[53] Este artículo, en relación con el artículo 18 de la Directiva (UE) 2016/680, establece que *"el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento a los que se hace referencia en los artículos anteriores se llevará a cabo de conformidad con las normas procesales penales cuando los datos personales figuren en una resolución judicial, o en un registro, diligencias o expedientes tramitados en el curso de investigaciones y procesos penales. Cuando los datos sean objeto de un tratamiento con fines jurisdiccionales del que sea responsable un órgano del orden jurisdiccional penal, o el Ministerio Fiscal, el ejercicio de los derechos de información, acceso, rectificación, supresión y limitación del tratamiento se realizará de conformidad con lo previsto en la Ley Orgánica 6/1985, de 1 de julio, en las normas procesales y en su caso, el Estatuto Orgánico del Ministerio Fiscal. En defecto de regulación del ejercicio de estos derechos en dichas normas, se aplicará lo dispuesto en esta Ley Orgánica".* Este precepto hace referencia a un régimen especial en cuanto al ejercicio de los derechos reconocidos, régimen que será estudiado al final del epígrafe.

[54] Vid. las Disposiciones Finales Segunda y Tercera de la Ley Orgánica 7/2021.

[55] En aras a la concisión, se ha resumido brevemente el contenido de los dos preceptos para focalizar la atención en el estudio pormenorizado de los ya mencionados derechos ARCO. Si bien en tales preceptos también se establece el derecho del interesado a acudir, por sí mismo o por representante, al responsable mediante la presentación de una solicitud. El responsable

Además, se incorpora la obligación del responsable de notificar a los destinatarios cuando se rectifique, suprima o limite el tratamiento de los datos a efectos de que estos también lo hagan, de manera que los datos sean exactos[56].

El artículo 25 por su parte indica que el interesado tiene la posibilidad de ejercer sus derechos mediante la autoridad de protección de datos competente en casos de aplazamiento, limitación u omisión de la información debiendo el responsable del tratamiento informar sobre esta previsión. La autoridad de protección de datos a que nos referimos deberá informar al interesado de todas las cuestiones necesarias.

A continuación, pasaremos a analizar cada uno de los derechos ARCO:

Derecho de acceso del interesado a sus datos personales

El derecho de acceso podría definirse como el derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le concierne y de, en caso de que se confirme el tratamiento, acceder a tales datos personales, así como a otra serie de información relativa a plazos, categorías especiales de datos o interesados en el tratamiento, entre otras más[57].

Vista esa definición no parece haber ninguna mayor complejidad en la comprensión del término más allá de qué información o datos debemos entender accesibles por parte del interesado. En esto la jurisprudencia comunitaria puede aportarnos cierta aclaración. Así, en primer lugar, se ha de decir que es doctrina consolidada del Tribunal de Justicia de la Unión Europea, desde la vigencia de la Directiva 95/46/CE, el considerar el derecho de acceso como requisito previo y necesario para ejercer los demás derechos[58]. Esto supone que, a priori, la

igualmente tiene el derecho a solicitar información complementaria si existen dudas razonables en relación con la identidad del solicitante. A este procedimiento es aplicable la normativa de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

[56] Relaciónese con el principio de exactitud y lealtad analizado.

[57] Vid. el extenso artículo 22

[58]de la Ley Orgánica 7/2021.

La STJUE de 7 de mayo de 2009, asunto Rijkeboer, C-553/07, se expresa en los siguientes términos: *"el citado derecho de acceso es indispensable para que el interesado pueda ejercer los derechos que se contemplan en el artículo 12, letras b) y c), de la Directiva, a saber, en su caso, cuando el tratamiento no se ajuste a las disposiciones de la misma, obtener del responsable del tratamiento de los datos, la rectificación, la supresión o el bloqueo de los datos [letra b)], o que proceda a notificar a los terceros a quienes se hayan comunicado los datos, toda*

extensión del derecho de acceso sea lo suficientemente amplia con el fin de, a posteriori, permitir el pleno y eficaz ejercicio de los derechos de rectificación y cancelación. En otras palabras, un derecho de acceso limitado restringiría los derechos de rectificación o cancelación.

Ahora bien, en contraste con esta amplitud, como acertadamente indica RODRÍGUEZ-MEDEL NIETO *"el hecho de que se refiera a datos personales tratados con ocasión de la prevención, detección, investigación y enjuiciamiento de infracciones penales justifica también que el contenido de la información que debe facilitarse sea notablemente inferior que en la regulación general prevista en el Reglamento*[59]*".* Evidentemente, el fin a que está llamada a regular la Ley Orgánica 7/2021 obliga a un derecho de acceso más limitado pues, como se dijo antes, el principio de consentimiento del interesado no existe en este ámbito por lo que tampoco se distingue entre aquella información aportada por el afectado como aquella información obtenida a partir de otros medios.

Por lo que respecta a cómo se ejerce el derecho, la Ley Orgánica 7/2021 es clara en este sentido. Declara el apartado 3 del artículo 22 que el derecho de acceso se entenderá cumplido cuando el responsable facilita al interesado cualquier sistema remoto, directo y seguro que garantice permanentemente el acceso a la totalidad de los datos. No obstante, si no se facilitara la totalidad de los datos, el interesado tendrá derecho a solicitar el resto. Por otra parte, si el interesado prefiere un medio distinto al suministrado por el responsable que suponga un coste desproporcionado, según la ley, el interesado deberá asumir el coste. En cualquier caso, el responsable deberá satisfacer el acceso sin dilaciones indebidas. Existe una pequeña excepción de la Directiva (UE) 2016/680 respecto del Reglamento (UE) 2016/679 que señala la autora anterior. La primera norma no prevé que el interesado obtenga copia ejercido el derecho de acceso a sus datos personales, mientras que la segunda norma sí lo prevé en su artículo 15[60].

---

rectificación, supresión o bloqueo efectuado, si no resulta imposible o supone un esfuerzo desproporcionado [letra c)]". Cfr. con la STC 292/2000 de 30 de noviembre, para la cual el acceso es el núcleo esencial del derecho reconocido en el art. 18.4 de la Constitución.

[59] Vid. RODRÍGUEZ MEDEL-NIETO, en ARAGÜENA FANEGO, C. y VIDAL FERNÁNDEZ, B (dir.), 2018: pág. 407.

[60] ARAGÜENA FANEGO, C y DE HOYOS SANCHO, M. (dir.), 2018: pág. 409. La Ley Orgánica 7/2021 no amplía en este aspecto el contenido mínimo de la Directiva (UE) 2016/680 por lo que el interesado carece del derecho a la obtención de copia en el ámbito de los fines de la ley.

Derecho de rectificación de los datos personales

Según VALLS PRIETO, el derecho de rectificación de los datos personales *"se podrá obtener por parte del responsable del tratamiento, sin que medie una dilación indebida, cuando los datos sean inexactos y en el caso de que sean incompletos que el interesado pueda solicitar que se completen[61]"*. De aquí se desprende, en mi opinión un doble derecho, o mejor dicho una doble manifestación del mismo derecho. Por un lado, el derecho a corregir los datos personales y, por otro lado, el derecho a completar los datos personales.

Este derecho es consecuencia lógica imprescindible si se quiere respetar el principio rector de exactitud del artículo 6.1.d) de la Ley Orgánica 7/2021 en relación con el apartado primero del artículo 23[62]. En la medida en que los datos deben ser exactos y actualizados, se debe dar la posibilidad del interesado de corregirlos o completarlos. De igual manera, se puede relacionar directamente el derecho de rectificación con el derecho de acceso e información de tal manera que, si se denegara el derecho de acceso e información, el afectado no tendría manera de corregir los datos personales que se consideran inexactos.

Con todo, y como claramente expresa la Ley Orgánica 7/2021, el interesado deberá concretar en la solicitud dirigida al responsable del tratamiento qué datos considera incorrectos y qué corrección habrá de hacerse acompañando la justificación pertinente. Si por el contrario es el responsable del tratamiento el que rectifica los datos personales inexactos que provienen de otra autoridad competente, deberá comunicarle la rectificación realizada como estipula el apartado 4 del artículo 23 de la Ley Orgánica 7/2021.

Derecho de cancelación o supresión *("al olvido") de los datos personales*

La Ley Orgánica 7/2021 define el derecho de cancelación o de supresión[63] en el apartado segundo del artículo 23 cuya dicción es la siguiente: *"el responsable*

[61] VALLS PRIETO, J. 2017: pág. 80. De conformidad con lo dicho por este autor, el derecho de rectificación de datos personales que se reconoce en la Directiva (UE) 2016/680 es de una extensión mucho mayor que el reconocido en la Decisión Marco 2008/977/JAI, consecuencia del instrumento empleado, pues la Decisión Marco no determinaba si el interesado podía ejercer su derecho de forma directa o mediante la autoridad nacional competente.

[62] Dice literalmente el precepto que *"el interesado tendrá derecho a obtener del responsable del tratamiento, sin dilación indebida, la rectificación de los datos personales que le conciernen, cuando tales datos resulten inexactos".*

[63] Es importante hacer una nota aclaratoria en este punto, pues tanto la doctrina como las autoridades en materia de protección de datos se refieren en numerosas ocasiones a este

del tratamiento, a iniciativa propia o como consecuencia del ejercicio del derecho de supresión del interesado, suprimirá los datos personales sin dilación indebida y, en todo caso, en el plazo máximo de un mes a contar desde que tenga conocimiento, cuando el tratamiento infrinja los artículos 6, 11 o 13, o cuando los datos personales deban ser suprimidos en virtud de una obligación legal a la que esté sujeto".

Atendiendo a la literalidad de la disposición observamos que la Ley Orgánica 7/2021 prevé, en primer lugar y para el caso en que el interesado no ejerza su derecho, un deber u obligación por parte del responsable del tratamiento, quien actuará de oficio –a iniciativa propia, según la ley– suprimiendo los datos personales de aquel; y en segundo lugar y para el caso en que el interesado ejerza su derecho, como un verdadero derecho que le asiste. Hecha esta breve aclaración, hemos de detenernos pormenorizadamente en este derecho y más aún por la materia que es objeto de estudio en este trabajo.

DE TERWANGNE asemeja el derecho al olvido con el derecho a ser olvidado[64]. Cierto es que desde el concepto creado en 1880 por el juez estadounidense Thomas Cooley, *"the right to be let alone"* o *"the right to be forgotten"* hasta la materialización en la década de los años 70 de *"le droit à l'oubli ou à l'effacement"* el objeto jurídico protegido, como indica DI PIZZO CHIACCHIO, no ha sido otro sino la dignidad de la persona y el libre desarrollo de su personalidad; pero un matiz importante que realiza este autor, en contraste con el anterior, es destacar la diferencia entre el *"the right to be forgotten"* respecto del *"the right to delete or to erasure"*, en español derecho a ser olvidado y derecho de supresión, o como hemos dicho popularmente "al olvido". El primero de ellos *"está centrado en una actitud que se espera de terceros"*, es decir que otras personas nos olviden u olviden nuestros datos, mientras que el segundo es *"una acción que se espera de uno mismo"*, siendo el propio interesado el que ejerce la acción[65].

---

derecho, desde una expresión más coloquial: *"el derecho al olvido"*, por tratarse de la facultad que tiene el interesado a que se olviden sus datos personales que han sido, son o van a ser objeto de tratamiento. Baste decir por el momento que cuando nos referimos al derecho de cancelación, supresión o al olvido estaremos refiriéndonos al mismo derecho.

[64] DE TERWANGNE, C. 2012: pág. 53: *"el derecho al olvido, también llamado derecho a ser olvidado es el derecho de las personas físicas a hacer que se borre la información sobre ellas después de un período de tiempo determinado".*

[65] DI PIZZO CHIACCHIO, A., 2018: págs. 69 a 77. Esta diferencia había sido ya teorizada por varios autores entre los que se destaca Paul A. BERNAL y Hans GRAUX.

Por otro lado, el derecho al olvido no debe entenderse como el derecho al anonimato[66], si bien, como argumenta DI PIZZO CHIACCHIO, hay algún autor que lo incorpora como un derecho subsidiario del derecho de supresión[67]. No obstante, considero no existe correlación entre un derecho al anonimato, o sea ser anónimo o desconocido frente a terceras personas, con un derecho al olvido o supresión de los datos personales que no significa implícitamente el desconocimiento absoluto del individuo máxime cuando existe el llamado proceso de seudonimización[68] y que posteriormente analizaremos jurisprudencialmente. Como concluye BERROCAL LANZAROT, el derecho de supresión se puede relacionar con *"la prescripción de oficio o a instancia de parte de los antecedentes penales, con la anonimización de las sentencias, con la amnistía y el indulto[69]".*

En relación con la afirmación de esta última autora, la anonimización, o seudonimización, de las sentencias que realiza un sistema como CENDOJ (Centro de Documentación Judicial) garantiza el derecho al olvido que ampara al afectado. Cuando leemos una sentencia de cualquier tribunal, no podemos discernir a quién se está dirigiendo el juzgador atendiendo exclusivamente a las partes y a los fundamentos de hecho y de derecho, pues la resolución judicial publicada pasa el anterior procedimiento de seudonimización[70]. En resumen, consiste en extraer la información que permite individualizar al individuo.

---

[66] DESGENS-PASANAU, G., 2016: pág. 141: *"il faut rappeler que droit à l'oubli ne signifie pas droit à l'anonymat".*

[67] DI PIZZO CHIACCHIO, A., 2018. pág. 72, en el pie de página nº124 referido a BERNAL Paul A. *"there is a close relationship between the two [deletion of data and anonymisation], and as and where it is technically posible the right of data deletion could be augmented with a form of subsidiary right – the right to have data anonymised".*

[68] Partiendo de la etimología griega del concepto: "nombre falso", el artículo 5.e) de la Ley Orgánica define la seudonimización como *"el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional se mantenga 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".* La seudonimización no implica *per se* el anonimato absoluto de la persona seudonimizada, pues sus datos únicamente se han "olvidado" de cara a terceras personas.

[69] BERROCAL LANZAROT, I., 2017: pág. 298.

[70] Si bien, como acertadamente señala la autora el procedimiento de seudonimización no ocurre respecto de las resoluciones del Tribunal Constitucional, el Tribunal Europeo de Derechos Humanos y el Tribunal de Justicia de la Unión Europea, pero baste ver cualquier resolución del CENDOJ para observar que numerosos datos personales como domicilio, DNI, nombre y apellidos, etc han sido suprimidos. Es cuanto menos curioso desde el punto de la lógica jurídica que los tribunales europeos, institución de donde proviene esta normativa, no prevea la seudonimización de sus resoluciones. BERROCAL LANZAROT, I., 2017. pág. 204.

Finalmente, en todo caso y respecto al procedimiento que establece la ley, la supresión debe hacerse sin dilaciones indebidas y a más tardar en el plazo de un mes desde que lo solicite el interesado, en los casos en que ejerza su derecho. El responsable, en el supuesto en que los datos personales del afectado deban conservarse a efectos probatorios o cuando este ponga en duda la exactitud de los mismos, limitará el tratamiento.

Derecho de oposición

Ni en la redacción de la Directiva (UE) 2016/680 ni en la redacción de la Ley Orgánica 7/2021 se hace referencia alguna al "derecho de oposición", a diferencia de la redacción tanto del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018. El derecho de oposición no es más que el derecho que asiste al interesado de impedir el tratamiento de sus datos personales. En ese caso, el responsable parará el tratamiento salvo que existan motivos legítimos imperiosos, según la redacción de la normativa general[71].

Ahora bien, el fin que persigue la normativa que es objeto de este trabajo no puede dejarse al albur de la voluntad del interesado. La investigación policial o judicial no puede suspenderse sino por algunas de las causas que establezca la normativa procesal criminal al efecto. Es por ello por lo que este derecho de oposición, realmente, no tiene cabida en la Directiva (UE) 2016/680 ni en la Ley Orgánica 7/2021.

RODRÍGUEZ-MEDEL NIETO afirma que existen otros derechos tales como el derecho a *"a presentar una reclamación, a la tutela judicial efectiva y a ser indemnizado en los daños y perjuicios sufridos*[72]*"*, los cuales se desprenderían de los artículos 52 y siguientes de la Directiva (UE) 2016/680 y 52 y siguientes de la Ley Orgánica 7/2021 del derecho a la tutela judicial efectiva frente a la autoridad de control o frente al responsable o encargado del tratamiento. Si bien no cabe duda que, se trata de potestades que reconoce la directiva y por tanto la ley, lo cierto es que ninguna novedad doctrinal añade el derecho a la tutela

[71] Vid. el artículo 18 de la Ley Orgánica 3/2018 en relación con el artículo 21 del Reglamento (UE) 2016/679.
[72] Vid. RODRÍGUEZ MEDEL-NIETO, en ARANGÜENA FANEGO, C. y DE HOYOS SANCHO, M. (dir.), 2018: pág. 410.

judicial efectiva por cuanto se trata de un derecho fundamental que reconoce directamente la Constitución en el artículo 24 a todos los ciudadanos.

Ejercicio de los derechos

Como se lleva diciendo desde el inicio de esta obra, la Directiva (UE) 2016/680 y la Ley Orgánica 7/2018 establecen una normativa especial en relación con la protección de datos abocadas al ámbito de investigación policial e instrucción penal, y como, de nuevo se repitió anteriormente, aquellas leyes no serán óbices para la aplicación normal de la normativa procesal penal. La Directiva (UE) 2016/680 establece un doble régimen para el ejercicio de estos derechos: el régimen general y el régimen especial, cuando se traten de datos incorporados en una causa penal[73].

En este extremo vamos a seguir a la autora RODRÍGUEZ-MEDEL NIETO quien constata que, en realidad, el contenido de los derechos ARCO no se ven afectados, sino la manera en que son ejercidos: *"si el tratamiento está vinculado a una investigación y a un proceso penal, el ejercicio de los derechos puede articularse a través de las normas de los Estados miembros, que serán normas procesales puesto que están vinculadas a la investigación y al proceso penal[74]".* Y es que la normativa procesal penal nacional ya regulaba con anterioridad a la entrada en vigor de la directiva algunos derechos relacionados con los datos personales. RODRÍGUEZ-MEDEL NIETO se interroga si tales normas por sí mismas eran suficientes antes de la entrada en vigor de la normativa actual respondiendo negativamente, pues la inexistencia de esta, argumenta, supondría que los afectados aplicarían la normativa general sin que la cláusula de restricción que se comenta a continuación llegue a entrar en aplicación.

Podemos destacar en este punto los artículos 301, 579 bis, 588 octies y 681 de la Ley de Enjuiciamiento Criminal[75]; e incluso de otra normativa relacionada al

[73] Como se dijo en la nota a pie de página número 48.

[74] Vid RODRÍGUEZ MEDEL-NIETO, en ARANGÜENA FANEGO, C. y DE HOYOS SANCHO, M., 2018: pág. 411.

[75] Como destaca la autora, el primer artículo decretaba el secreto, ahora la "reserva" de las diligencias del sumario hasta el juicio oral; el segundo artículo acerca de la utilización de la información obtenida en un procedimiento distinto y descubrimientos causales; respecto del tercer precepto se establece la posibilidad del Ministerio Fiscal o de la Policía Judicial de requerir a cualquier persona, que deberá guardar secreto, la conservación y protección de datos hasta que se obtenga la autorización judicial para su cesión con un período máximo de 90 días

respecto tal y como el artículo 2 de la Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales[76]; los artículos 138.2 y 140.3 de la Ley de Enjuiciamiento Civil[77], de aplicación supletoria respecto del derecho procesal penal; el artículo 16 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia; o el artículo 234 y siguientes de la Ley Orgánica 6/1985 del Poder Judicial[78], modificados por la entrada en vigor de la Ley Orgánica 7/2021.

Límites a los anteriores derechos

Hay que aclarar que los derechos anteriores que han sido analizados no son derechos absolutos y que su ejercicio puede suponer límites siempre que estén debidamente previstos por la normativa y su restricción tenga cabida por estar justificada. A esto se refiere el artículo 24 de la Ley Orgánica 7/2021 cuando autoriza al responsable a *"aplazar, limitar u omitir la información del artículo 21.2, así como denegar total o parcialmente los derechos de los artículos 22 y 23".*

Fíjese en que la Ley estipula que tal restricción deberá realizarse salvando los derechos fundamentales e intereses del afectado, cuando resulte necesario y de manera proporcional para la consecución de ciertos fines tales como impedir la obstaculización de investigaciones policiales o judiciales, proteger la seguridad pública, la Seguridad Nacional o los derechos y libertades de terceros.

Señala RODRÍGUEZ-MEDEL NIETO, que la Directiva (UE) 2016/680, y con ella la Ley Orgánica 7/2021, se diferencia del Reglamento (UE) 2016/679 en que aquella permite a los Estados miembros una cláusula de restricción, ya sea total

prorrogables hasta 180. Finalmente, el cuarto precepto establece ciertas medidas a decidir por el tribunal para proteger la identidad de la víctima y su familia.

[76] El precepto faculta al juez la adopción de decisiones que limitaran el acceso a los datos personales de testigos y peritos con el fin de preservar su identidad.

[77] Estos preceptos facultan al juzgador a decidir mediante auto atribuir carácter reservado a las actuaciones cuando resulten necesarias.

[78] El precepto dispone que "*los Letrados de la Administración de Justicia y funcionarios competentes de la oficina judicial y de la oficina fiscal facilitarán a los interesados cuanta información soliciten sobre el estado de las actuaciones procesales, que podrán examinar y conocer, salvo que sean o hubieren sido declaradas secretas o reservadas conforme a la ley. Las partes y cualquier persona que acredite un interés legítimo y directo tendrán derecho a obtener, en la forma dispuesta en las leyes procesales y, en su caso, en la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, copias simples de los escritos y documentos que consten en los autos, no declarados secretos ni reservados. También tendrán derecho a que se les expidan los testimonios y certificados en los casos y a través del cauce establecido en las leyes procesales".*

o parcial, de los derechos ARCO y que son las que acabamos de mencionar previamente. Siguiendo a la misma autora, tal cláusula tiene un triple efecto, a saber:

- Servir como cláusula de exclusión, denegándose el acceso a los datos si facilitándolo se pone en peligro el derecho o libertad de un tercero.
- En relación con el fin de la solicitud de información, omitirse los motivos por los que se deniega si se protege aquel fin.
- Dar una especial legitimación a la autoridad de protección de datos ejerciendo los derechos ARCO en nombre del interesado debiendo informarle. Se restringe el acceso directo por parte del interesado, pero no indirecto por vía de la autoridad de datos[79].

En resumen, estos límites existen principalmente por la confrontación con otros derechos dignos de tuición es por ello por lo que habrá que desplegar una actuación de ponderación y proporcionalidad de derechos para discernir cuál de ellos debe prevalecer siguiendo la doctrina que a tal efecto ha elaborado el Tribunal Constitucional[80]. Un claro ejemplo es el que nos aporta ESPÍN TEMPLADO en relación con la libertad de información la cual, siguiendo la Sentencia del Tribunal Constitucional 58/2018, debe ceder frente a los derechos de la personalidad dentro de los que se enmarcan la protección de datos[81].

VI. Responsable y encargado del tratamiento. La figura del delegado de protección de datos en la Ley Orgánica 7/2021. Autoridades independientes.

Nos compete ahora tratar las personas encargadas de aplicar la Ley Orgánica 7/2021, estas son, aquellas que se encargan de que los objetivos de los artículos 1 y 2 se cumplan de manera efectiva que como ya vimos son las autoridades competentes que se prevén en el artículo 4. Esta materia se encuentra en el Capítulo IV de la Ley que comprende los artículos 27 a 42, si bien vamos a

[79] Vid. RODRÍGUEZ MEDEL-NIETO, en ARANGÜENA FANEGO, C. y DE HOYOS SANCHO, M. (dir.), 2018: pág. 406.
[80] Vid. la reflexión de SÁNCHEZ GONZÁLEZ en relación con la evolución y aplicación del juicio de ponderación y proporcionalidad por parte del Tribunal Constitucional a lo largo de su historia. Se mencionan entre otras las SSTC 31/1981, de 28 de julio, y 53/1985, que sirvieron de pilar fundamental para la teorización del criterio actual. SÁNCHEZ GONZÁLEZ, S., 2003: págs.11-16.
[81] LOPEZ GUERRA, L., ESPÍN TEMPLADO, E. y VV.AA., 2018: pág. 220.

analizar, por la relevancia que tienen sus resoluciones, a las autoridades de protección de datos independientes ex Capítulo VI que comprende los artículos 48 a 51. Este estudio conjunto se debe por lo dispuesto en el artículo 34 el cual dice que *"el responsable y el encargado del tratamiento cooperarán con la autoridad de protección de datos competente, en el marco de la legislación vigente, cuando esta lo solicite en el desempeño de sus funciones"* y 36 de la ley, el cual establece la posibilidad de que el responsable y el encargado consulten a la autoridad de protección de datos sobre el tratamiento a realizar en circunstancias extraordinarias que decreta la ley, estas son:

- Cuando la evaluación de impacto en la protección de los datos indique que el tratamiento entrañaría un alto nivel de riesgo[82], a falta de medidas del responsable para minimizar los posibles daños.
- Cuando el tipo de tratamiento pueda generar un alto nivel de riesgo para los derechos y libertades de los interesados, en particular, cuando se usen tecnologías, mecanismos o procedimientos nuevos[83].

La autoridad de protección de datos, si advierte que efectivamente existe riesgo de que el tratamiento no cumpliese lo dispuesto en la ley, en seis semanas, prorrogables un mes, desde la consulta, asesorará al responsable y encargado. Si, transcurrido el plazo no se ha obtenido respuesta, el tratamiento consultado se considerará lesivo para los derechos y libertades del interesado. Como dice la disposición, *"no operará la presunción del carácter favorable del mismo".*

Dicho esto, antes de comenzar a hablar de cada uno de ellos, hemos de distinguir las figuras del responsable y encargado del tratamiento, términos que pueden conducir a confusión. La distinción la da la propia Ley Orgánica 7/2021 en el artículo 5 aparatados g) y h). A estos efectos, el responsable del tratamiento es cualquier autoridad competente del artículo 4 –las Fuerzas y Cuerpos de

[82] La Agencia Española de Protección de Datos define riesgo: "*la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. El nivel de riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo. Las amenazas y los riesgos asociados están directamente relacionados, en consecuencia, identificar los riesgos siempre implica considerar la amenaza que los puede originar."* Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD, Madrid, 2018: pág. 4.

[83] La evaluación de impacto se refiere al estudio que deberá realizar el responsable cuando considere que un tratamiento de datos puede suponer un alto riesgo para los derechos y libertades del afectado por emplear nueva tecnología o cualquier otro nuevo mecanismo. Vid. el artículo 35 de la Ley.

Seguridad del Estado, las Administraciones Penitenciarias, el Ministerio Fiscal, etcétera.– que, por sí sola o junto con otra, establece los fines y medios del tratamiento de los datos personales del afectado, mientras que el encargado del tratamiento es aquella persona, física o jurídica, autoridad pública, servicio o cualquier otro organismo que trata datos personales por cuenta del responsable del tratamiento. El responsable del tratamiento es, valga la redundancia, quien tiene la responsabilidad de que se cumplan todas las previsiones hechas hasta ahora[84], de hecho, solo basta leer las disposiciones de la ley para observar la prevalencia del responsable sobre el encargado, pues la redacción de la norma repite en mayor número el término responsable y en menor medida el término encargado. Ahora bien, esto no significa que el encargado no tenga ninguna responsabilidad, sino todo lo contrario. Deberá acogerse a las funciones que la ley le atribuye, pues en caso contrario, será considerado responsable con respecto al tratamiento de que se trate[85].

Responsable del tratamiento

El artículo 27 de la Ley Orgánica 7/2021 establece las obligaciones del responsable del tratamiento que, como se ha dicho, deberá tener en consideración la naturaleza, ámbito, fines y niveles de riesgo para los derechos y libertades del afectado para garantizar que el tratamiento se lleve a cabo conforme los cauces legales empleando las medidas técnicas y organizativas necesarias para ello. Estas medidas técnicas y organizativas que debe articular el responsable del tratamiento se encuentran desarrolladas en el siguiente precepto de la protección de datos desde el diseño y por defecto[86]. Esto quiere decir que el responsable deberá tomar las decisiones necesarias (por diseño), o

[84] Vid. el preámbulo de la Ley Orgánica 7/2021 la cual dice que El responsable del tratamiento, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los niveles de riesgo para los derechos y libertades de las personas físicas, aplicará las medidas técnicas y organizativas apropiadas

[85] Vid. el apartado 4 del artículo 30 de la Ley Orgánica 7/2021.

[86] El Supervisor Europeo de Protección de Datos lo define de la siguiente manera: *"the design shall be identified as taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the processing as well as the risks for the rights and freedoms of those individuals. By default, only personal data that are necessary for each specific purpose of the processing may be processed".* Opinion 5/2018 adopted on 31st May on Preliminary Opinion on privacy by design, 2018, pág. 5.

no tomarlas (por defecto), con el fin de no lesionar ni los principios rectores ni el contenido de los derechos de la ley[87].

Según el artículo 32, el responsable llevará por escrito, incluyendo el formato digital, un registro de las actividades del tratamiento, llamado por la doctrina con el acrónimo RAT[88], que deberá estar a disposición de la autoridad de protección de datos. El RAT debe incorporar cierta información tal como y sin ánimo exhaustivo la identificación del responsable, y en su caso del corresponsable ex artículo 29, y del delegado de protección y sus datos de contacto, los fines del tratamiento, descripción de las categorías de interesados y de datos, la base jurídica del tratamiento, los plazos y la descripción de las medidas técnicas y organizativas que respecto del tratamiento ha adoptado el responsable. Este registro deberá ser publicado por vía electrónica y estará a disposición de la autoridad de protección de datos.

Lo mismo se desprende respecto del artículo 33 en relación con las operaciones de tratamiento automatizado como la recogida, alteración, consulta, comunicación, transferencias y combinación o supresión de datos. El fin de este registro no es más que el de controlar la legalidad del tratamiento y deberá estar a disposición de la autoridad de protección de datos competente a solicitud de esta. En este extremo, están obligados tanto encargado como responsable.

Encargado del tratamiento

Siguiendo al artículo 30, el encargado podrá ser una persona física o jurídica, pública o privada, vinculada al responsable por medio de un contrato o cualquier instrumento jurídico, cuyo clausulado contendrá la duración, el tipo de datos a tratar, la finalidad, las instrucciones de actuación y demás garantías en caso de

[87] El artículo 28 incorpora una cláusula *in fine* en virtud de la cual se dice que *las medidas garantizarán, por defecto, que los datos personales no sean accesibles a un número indeterminado de personas sin intervención humana".* Cfr. con el artículo 14 por cuanto se prohíben las decisiones basadas en un tratamiento automatizado que produzca efectos lesivos para el interesado con la excepción de que se autorice por ley o por el derecho de la Unión, en cuyo caso se debe incluir el derecho a obtener la intervención humana en la revisión de la decisión. Fíjese que en relación con las categorías especiales de datos existe una excepción especial por cuanto no se permiten las decisiones automatizadas salvo que se salvaguarden los derechos y libertades del afectado.

[88] NÚÑEZ GARCÍA dice que *"[…] uno de ellos es la llevanza de un registro de actividades de tratamiento (RAT), recogida con gran detalle en el artículo 30 del RGPD".* RALLO LOMBARTE, A. (dir.), 2019: pág. 365.

incumplimiento de sus funciones y deberes de confidencialidad, asistencia e información.

En relación con esta figura poco podemos añadir más que la obligación de también llevar un registro si bien con un contenido menor debido lógicamente a que actúa por cuenta del responsable y no por sí mismo, como se desprende del artículo 32.2. El contenido del RAT que corresponde al encargado deberá contener la información relativa al nombre y datos de contacto del encargado/s, del responsable en cuyo nombre actúe y del delegado de protección de datos, así como las categorías de tratamientos efectuados, las transferencias de datos a un Estado no miembro de la Unión o a una Organización Internacional, identificándolos debidamente cuando el responsable lo ordene, y las medidas técnicas y organizativas adoptadas.

Delegado de protección de datos

Dispone el artículo 40 de la Ley que la figura del delegado de protección de datos deberá ser designada en todo caso por el responsable del tratamiento, exceptuando a los órganos jurisdiccionales y al Ministerio Fiscal, para quienes no existe tal obligación siempre que el tratamiento se refiera a sus funciones jurisdiccionales. El artículo 42 establece sus funciones mínimas las cuales son: informar y asesorar al responsable del tratamiento acerca de las obligaciones que les incumben en virtud de la ley y de otras disposiciones de protección de datos aplicable; supervisar el cumplimiento de lo dispuesto en esta ley, así como de lo establecido en las políticas del responsable del tratamiento en materia de protección de datos personales y las auditorías correspondientes; ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su realización; cooperar con la autoridad de protección de datos; actuar como punto de contacto de la autoridad de protección de datos realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos es una figura necesaria y será elegido en función de sus conocimientos y cualidades profesionales requiriéndose incluso certificación profesional. Según el artículo 41 de la Ley el delegado no podrá ser removido ni sancionado ni por el responsable ni por el encargado salvo dolo o negligencia. DURÁN CARDÓ resume a la perfección la labor del delegado de protección de datos en los siguientes términos: *"[…] el delegado de protección*

de datos deberá intentar alinear ambos objetivos y crear una auténtica cultura de cumplimiento, en la que todas las piezas del puzle existan y encajen a la perfección, cumpliendo cada una de ellas con el papel que se le hubiera asignado[89]*".*

Autoridades de protección de datos independientes

Hasta el momento se ha estado hablando de la Agencia Española de Protección de Datos como autoridad nacional en la materia, pero no es la única. En el capítulo VI de la Ley Orgánica 7/2021 se regulan las llamadas Autoridades de Protección de Datos Independientes. El artículo 48 dice cuáles son estas autoridades: la Autoridad Española de Protección de Datos, quien representará a la Nación en el Comité Europeo de Protección de Datos, y las autoridades autonómicas de protección de datos[90], por supuesto exclusivamente respecto de los tratamientos de que sean responsables de conformidad con su título competencial. Esta última cuestión en relación con el ámbito competencial entre las autoridades de control nacionales y autonómicas no ha estado exenta de problemas desde la aprobación de la Ley Orgánica 5/1992. De las polémicas doctrinales y jurisprudenciales al respecto a lo largo de estos años, MURILLO DE LA CUEVA concluye que *"todo tratamiento que se lleve a cabo por una administración o entidad del sector público autonómico con ocasión del ejercicio de funciones públicas […] queda bajo la competencia de las autoridades autonómicas de control con independencia de la forma jurídica que aquellas adopten y de que su actuación se desarrolle bajo la veste jurídico pública o con sujeción total o parcial al derecho privado*[91]*".*

Así, las autoridades de protección de datos tienen potestades de investigación, de advertencia y control de lo dispuesto en la normativa, de sanción de las infracciones cometidas, de elaboración de recomendaciones, de órdenes de rectificación, supresión, limitación y prohibición del tratamiento, de

[89] Vid. DURÁN CARDÓ, en TRONCOSO REIGADA, A. (Dir.), 2021: pág. 2334.
[90] Actualmente existen la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía. En la actualidad podrían sumarse otras autoridades de control en las comunidades de Aragón, Islas Baleares y Castilla y León tras la reforma de sus respectivos estatutos de autonomía.
[91] Vid. MURILLO DE LA CUEVA, en TRONCOSO REIGADA, A. (dir.): 2021, pág. 2662.

asesoramiento mediante la publicación de informes y dictámenes, así como de comunicar cualquier vulneración de la seguridad[92].

Como manifestación de las anteriores potestades, las autoridades tienen las siguientes funciones: supervisar y hacer cumplir las disposiciones adoptadas con arreglo a esta ley; promover la sensibilización y la comprensión de la ciudadanía acerca de los riesgos, normas, garantías y derechos relativos al tratamiento; asesorar a las Cortes Generales, al Gobierno de la Nación y a los organismos dependientes o vinculados a la Administración General del Estado, así como, de acuerdo con su ámbito competencial, a las Asambleas Legislativas de las comunidades autónomas, los Consejos de Gobierno y los organismos dependientes o vinculados a la Administración de las comunidades autónomas, acerca de las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento; promover la sensibilización de los responsables y encargados del tratamiento en relación con las obligaciones que les incumben; facilitar la información solicitada por los interesados sobre el ejercicio de sus derechos en virtud de esta ley y, en su caso, cooperar a tal fin con las autoridades de protección de datos de otros Estados miembros de la Unión Europea; tramitar y responder las reclamaciones presentadas por un interesado o por una entidad, organización o asociación de conformidad con el artículo 55, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable; controlar, de acuerdo con lo dispuesto en el artículo 25, la licitud del tratamiento e informar al interesado en un plazo razonable sobre el resultado del control o sobre los motivos por los que no se ha llevado a cabo; cooperar, en particular compartiendo información, con otras autoridades de protección de datos y prestarse asistencia mutua; llevar a cabo investigaciones sobre la aplicación de esta ley, en particular basándose en la información recibida de otra autoridad de protección de datos u otra autoridad pública; realizar un seguimiento de acontecimientos que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, de manera concreta sobre el desarrollo de las tecnologías de la información y la comunicación; prestar asesoramiento sobre las operaciones de tratamiento

[92] Artículo 50 de la Ley Orgánica 7/2021.

contempladas en el artículo 36; contribuir a las actividades del Comité Europeo de Protección de Datos; informar todas las disposiciones legales o reglamentarias que afecten a tratamientos sometidos a esta ley. Estas funciones son completamente gratuitas para el interesado y el delegado de protección de datos. Finalmente, el artículo 51 establece el principio de asistencia mutua en virtud del cual las autoridades de protección de datos de los distintos estados miembros están obligadas a cooperar y facilitar la información requerida por las autoridades de otros estados miembros, sin dilaciones indebidas a más tardar en el plazo de un mes desde que son requeridas. Las solicitudes no podrán denegarse, a no ser que la autoridad española no sea competente por la normativa nacional o comunitaria, y serán gratuitas salvo circunstancias excepcionales[93].

Los capítulos VII, de las reclamaciones, y VIII, del régimen sancionador, únicamente estipulan los distintos procedimientos en caso de exigir una reclamación o ser sancionado por parte de la autoridad de protección de datos[94].

VII. Transferencia de datos a terceros estados no miembros de la Unión Europea. Deber de colaboración del artículo 7.

En el Capítulo V, artículos 43 a 47, la Ley Orgánica 7/2021 habla sobre las transferencias de datos a terceros estados no miembros de la Unión y a Organizaciones Internacionales. Ni la Directiva ni la Ley dan un concepto acerca de lo que debe entenderse por "transferencia de datos" más allá de la STJUE de 6 de octubre, asunto Schrems, C-362/14 que lo incorporaba como un tipo de tratamiento, siendo la doctrina y las autoridades las encargadas de definirlo. Así, siguiendo a HERRÁN ORTIZ, podemos definir la transferencia de datos personales como *"cualquier movimiento de datos personales desde un responsable o encargado en territorio de la UE fuera del Espacio Económico de la UE[95]",* lo cual significa que las transferencias de datos entre Estados miembros

[93] Vid. el artículo 51 de la Ley.

[94] Las disposiciones contenidas en estos capítulos no tienen mayor importancia doctrinal. No compete tratar una por una los distintos tipos de reclamaciones, infracciones y sanciones por cuanto no tienen mayor dificultad. La simple lectura de los preceptos nos informa del régimen aplicable.

[95] Vid. HERRÁN ORTIZ, en TRONCOSO REIGADA, A. (Dir.), 2021: pág. 2537. En lo que respecta al EEE, el Espacio Económico Europeo lo integran los 27 países de la Unión Europea además de Liechtenstein, Noruega e Islandia.

del Espacio Económico Europeo no se rigen por las siguientes líneas, sino por la Disposición Adicional Segunda de la Ley Orgánica 7/2021 que recoge una regulación más laxa, pues aquella no estará limitada o prohibida por motivos relacionados con la protección de las personas físicas respecto al tratamiento de sus datos.

En cualquier caso, el artículo 43 de la Ley exige que las transferencias de datos extra-Unión Europea cumplan una serie de condiciones: que sean necesarias para los fines de la ley; que los datos se transfieran a una autoridad competente; que, en su caso, se permita la transferencia ulterior[96]; y que la Comisión Europea haya adoptado una decisión de adecuación del nivel de protección de datos personales respecto del Estado receptor de la transferencia. Esto nos plantea un interrogante. ¿Qué debe entenderse por un nivel adecuado de protección de datos? SÁNCHEZ DOMINGO constata que estamos ante un concepto jurídico indeterminado para cuya concreción se debe acudir a lo dispuesto por el Grupo de Trabajo del Artículo 29[97]. Siguiendo a esta misma autora, los criterios que establece el Grupo de Trabajo son unas *"condiciones mínimas como punto de partida"* entre las que se encuentran por ejemplo el hecho de ofrecer un correcto cumplimiento de las normas de protección de datos por parte de los responsables, permitir el ejercicio eficaz de los derechos de protección de datos de los interesados y reconocer el derecho de recurso a los perjudicados. La Comisión Europea ha reconocido como países o territorios con un nivel de protección adecuado a Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda[98]. En resumen de todo lo anterior, estos territorios deben reconocer una protección *"esencialmente equivalente"* al de la Unión, por emplear términos literales de la autora SÁNCHEZ DOMINGO.

[96] Esta es, la transferencia de datos obtenidos de un Estado miembro o no a otro no miembro.

[97] SANCHEZ DOMINGO, M.B. 2017: pág. 25. Vid. el Documento de trabajo WP12 sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de la Unión Europea sobre protección de datos. Aprobado por el Grupo de Trabajo del Artículo 29, el 24 de julio de 1998.

[98] También se reconoció a Estados Unidos, aunque el Tribunal de Justicia de la Unión Europea invalidó la Decisión 2016/1250, de 12 de julio de 2016, de la Comisión mediante la STJUE de 16 de julio de 2020, asunto Facebook Ireland y Schrems, C-311/18 por considerar que el país no aseguraba un nivel de protección adecuado.

Ahora bien, la normativa permite la transferencia de datos personales a terceros países aun cuando no exista ese nivel de adecuación mínimo que exige la Comisión. Es el caso de los artículos 45 y 46 de la Ley.

El primer precepto hace referencia a la transferencia de datos a terceros estados no miembros cuando existan garantías de protección suficientes y concretadas. Garantías que pueden quedar acreditadas mediante dos vías: bien un instrumento jurídicamente vinculante –según el artículo 39.2 de la Directiva (UE) 2016/680, este instrumento puede ser cualquier acuerdo internacional bilateral o multilateral en vigor entre los Estados miembros y terceros países– o mediante una evaluación positiva de las medidas de protección de datos personales del Estado receptor por parte del responsable del tratamiento. Esta evaluación debería entenderse como la observación y análisis diligente de las normas relativas a la protección de datos personales del destinatario, análisis que habrá de realizar el emisor de la transferencia. De concluirse una evaluación positiva, esto es, que se reconozca esa protección *"esencialmente equivalente al de la Unión"* se permitirá la transferencia[99].

El artículo 46, por otra parte, recoge la regulación en caso de ausencia de la autorización de la Comisión Europea o en caso de falta de instrumento aplicable o evaluación negativa por parte del responsable a que hacía referencia el artículo anterior. Lo cierto es que esta disposición se refiere a circunstancias absolutamente excepcionales y necesarias permitiendo la transferencia de datos personales a terceros estados no miembros para proteger bien los derechos y libertades del interesado bien los de la comunidad. De nuevo, se exige que esta transferencia quede documentada y a disposición de la autoridad de protección de datos competente. Eso sí, el precepto establece en su párrafo segundo una disposición imperativa de protección del interesado, pues se dice literalmente que *"los datos personales no se transferirán, si la autoridad competente de la transferencia determina que los derechos y libertades fundamentales del interesado prevalecen sobre el interés público en la transferencia".* Se priman de esta manera los derechos y libertades individuales sobre los colectivos siempre

[99] En este caso, la transferencia se deberá documentar e informar de ella a la autoridad de protección de datos personales incluyendo la fecha, hora y justificación de la transferencia, información sobre la autoridad competente destinataria y los datos transferidos.

que, atendiendo a las circunstancias y al contexto en que se realiza la transferencia, ello sea necesario.

Hasta aquí, las transferencias a que se hacía referencia anteriormente siempre eran entre autoridades competentes, si bien, la Ley Orgánica 7/2021 recoge la posibilidad de realizar transferencias de datos a un destinatario no autoridad competente de un Estado no miembro. Nos referimos al artículo 47 que establece una posibilidad que podríamos calificar de *"ultraextraordinaria"* que se daría, literalmente dispone el precepto, *"excepcionalmente, en casos particulares y específicos y sin perjuicio de la existencia de un acuerdo internacional"*. El precepto exige que se cumplan ciertos requisitos para poder realizar este tipo de transferencia tales como cumplir las disposiciones la propia Ley, que la transferencia se documente y se informe a la autoridad competente (entendemos a la autoridad competente del Estado miembro emisor) y que se cumplan todas las condiciones siguientes[100]:

- Que la transferencia sea estrictamente necesaria para la realización de una función de la autoridad competente que lleva a cabo la transferencia conforme al Derecho de la Unión Europea o a la legislación española, con cualquiera de los fines del artículo 1.
- Que la autoridad competente que realiza la transferencia determine que ninguno de los derechos y libertades fundamentales del interesado es superior al interés público que precise de la transferencia de que se trate.
- Que la autoridad competente que realiza la transferencia considere que la transferencia a una autoridad competente del Estado en el que está establecido el destinatario, con cualquiera de los fines del artículo 1, resultaría ineficaz o inadecuada, en particular porque la transferencia no pueda efectuarse dentro de plazo.
- Que se informe sin dilación indebida a la autoridad competente para los fines que contempla el artículo 1 de dicho Estado, salvo que esto resulte ineficaz o inadecuado.

[100] Cfr. con los artículos 45 y 46 con el artículo 47 de la Ley. Al tratarse de una transferencia directa a un destinatario no autoridad competente, la normativa comunitaria exige que se cumplan todas y cada una de las condiciones que se mencionan con el fin de proteger al máximo los derechos del interesado.

- Que la autoridad competente que realiza la transferencia informe al destinatario de la finalidad o finalidades específicas para las que puede tratar los datos personales, siempre y cuando dicho tratamiento sea necesario.

Finalmente es importante decir que la preceptiva documentación e información a las autoridades de control competentes de los artículos 45, 46 y 47 se realiza a posteriori, es decir, después de haberse realizado la transferencia. SÁNCHEZ DOMINGO destaca que, si bien la normativa es garantista y ofrece una protección del interesado satisfactoria, una intervención a priori de la autoridad competente ofrecería aún mayores garantías para los ciudadanos. En sus palabras, *"[…] en ambos casos, la intervención de la autoridad de supervisión es posterior a la transmisión. Su participación en un momento anterior supondría una mayor garantía para los ciudadanos*[101]*".*

No se nos puede olvidar la importantísima relevancia del artículo 7 de la Ley Orgánica 7/2021 que recoge un deber de colaboración tanto de las Administraciones públicas como de las personas físicas y jurídicas para con las autoridades judiciales y policiales cuando estas soliciten datos o informes que sean necesarios para los fines de la propia ley, y siempre recabándose autorización judicial cuando legalmente sea exigible. El apartado 4 del precepto recoge una cláusula excepcional en contraste con el deber de colaboración que se recoge en la Ley Orgánica 3/2018 pues, a diferencia de esta, el interesado no será informado de la transmisión de sus datos con el fin de garantizar la correcta prosecución de la actividad investigadora.

VIII. Conclusiones.

Una vez llegado hasta aquí se tendrán diversos interrogantes respecto de diversas cuestiones de la normativa que merecen una respuesta, si no concluyente o irrefutable, sí reflexiva y debatible. Antes de todo, habrá que preguntarse el porqué de la normativa. La respuesta la tenemos desde diciembre de 2007, cuando se firmó el Tratado de Lisboa. Desde entonces, la Unión se arrogó funciones que correspondían previa y plenamente a la soberanía de los Estados miembros. Hablamos del Título V, Capítulo IV y V de la cooperación

[101] SANCHEZ DOMINGO, M.B. 2017: pág. 35.

judicial y policial en materia penal del Tratado de Funcionamiento de la Unión Europea, más en concreto los artículos 83 y 87. De esta manera, se han creado agencias europeas tales como Eurojust y Europol, en el ámbito judicial penal y policial, respectivamente, cuya finalidad es la cooperación entre los Estados miembros en la persecución de delitos[102] que se cometen *intra-Schengen* sirviéndose de la normativa de trasposición. Como dicta TRONCOSO REIGADA, *"la Directiva 2016/680, al mismo tiempo que pretende llevar a cabo una primera armonización normativa en Protección de Datos personales en un ámbito que hasta ahora pertenecía a la soberanía de los Estados y que estaba regulado por la Decisión Marco 2008/977/JAI del Consejo, tiene también la voluntad decidida de facilitar la compartición de información policial, mejorando la eficacia policial ante un desafío terrorista que no tiene en cuenta las fronteras nacionales y cuyos autores se mueven libremente en el espacio Schengen[103]".*

Pero dicho esto nos surge el *quid* de la cuestión. ¿Ha funcionado esta normativa en el Espacio de Libertad, Seguridad y Justicia de la Unión? O, en otras palabras, ¿ha facilitado la persecución de delitos la nueva normativa en comparación a la anterior?

Antes de responder a estas preguntas, es importante mencionar que la Comisión Europea publicó en enero de 2016 un *factsheet* en relación a cómo la nueva reforma de protección de datos[104] ayudaría a luchar contra el crimen internacional. El factsheet destacaba dos ideas: el ahorro de tiempo, de dinero, el reforzamiento de la cooperación internacional, así como las garantías y límites reconocidos por la Unión[105]. Desde luego, por cuanto se ha analizado previamente es innegable el encomiable balance entre libertades y derechos

[102] Vid. los delitos mencionados en el artículo 83 del Tratado de Funcionamiento de la Unión Europea, entre ellos el delito de terrorismo, blanqueo de capitales, etc. Nótese en que los delitos referidos tienen un componente transfronterizo.
[103] TRONCOSO REIGADA, A. (Dir.). 2021: pág. 181.
[104] En este documento la Comisión se refería al paquete legislativo que se acabaría aprobando en abril de aquel mismo año y que como ya hemos dicho estaría compuesto por el Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680.
[105] Factsheet of the European Commission adopted in January 2016, *how will the Data Protection reform help fight international crime?* El documento dice literalmente *"under the new Directive, everyone's personal data must be processed lawfully, fairly, and only for a specific purpose, a purpose that is always linked to the fight against crime. The Directive ensures that personal data processing across the EU complies with the principles of legality, proportionality, and necessity, with appropriate safeguards for individuals. It also ensures completely independent supervision by national data protection authorities, and effective judicial remedies".*

individuales y colectivos que realiza el legislador comunitario en este aspecto, prohibiendo o limitando el tratamiento cuando prevalezcan los intereses del interesado sobre los públicos y dotando a aquel de un elenco de derechos cuya lesión podrá invocar ante los tribunales.

Ahora bien, independientemente de todo esto, volvemos a las cuestiones anteriores. ¿Ha surtido efecto o no la nueva regulación? Como se dijo justo en el párrafo anterior, si el objetivo de la reforma era ahorrar tiempo, dinero y reforzar la cooperación internacional, podemos concluir con un rotundo sí. Si bien, en España, la tardía trasposición de la Directiva (UE) 2016/680 –por la que fuimos, una vez más, condenados por el Tribunal de Justicia de la Unión Europea[106]– supuso la tardía entrada en vigor de la Ley Orgánica 7/2021, máxime cuando su completa entrada en vigor fue a finales de noviembre de 2021[107], y por ello los efectos de la normativa aún no se han manifestado de forma clara y notoria, a diferencia de otros Estados miembros. Así, tras dar una respuesta afirmativa, hay que aportar las siguientes pruebas de que efectivamente la normativa ha surtido el efecto pretendido.

En primer lugar, atendiendo al *Annual Report* 2020 de Eurojust el número de casos que se han tramitado en el seno de esta agencia europea se ha incrementado exponencialmente desde 2016, como se desprende del gráfico que se adjunta en el anexo final. En efecto, la nueva normativa armonizadora ha permitido la cooperación, en este caso entre autoridades judiciales del orden penal, para la prosecución de delitos transfronterizos mediante un procedimiento eficaz, sumario y sin costes. Siguiendo el mismo *Report* del año 2020, la mayoría de estos delitos eran de ámbito económico fraudes, estafas, y blanqueo de capitales, además de delitos de tráfico de drogas, de personas, de terrorismo y cibercrímenes.

Europol, por otro lado, cuenta con tres sistemas distintos de intercambio de información con países miembros y no miembros de la Unión. Estos sistemas de intercambio de información son el SIENA (*Secure Information Exchange Network Application*), el EIS (*Europol Information System*) y el EPE (*Europol Platform for*

[106] Vid. la STJUE de 25 de febrero de 2021, asunto Comisión Europea v. Reino de España, C-658/19.
[107] Vid. la Disposición Final Duodécima de la Ley Orgánica 7/2021.

Experts). Hay que decir que, si bien estos sistemas de intercambio de información se crearon al amparo de la normativa derogada, la normativa actualizada ha dotado de mayor flexibilidad de actuación a Europol al facilitar la transmisión de datos entre países[108].

Como ejemplo de lo anterior, y sin ánimo exhaustivo, podemos mencionar un caso de tráfico de drogas cuya investigación inicial comenzó en Rumanía y envolvía a otros países comunitarios. Las autoridades rumanas solicitaron un traspaso de información vía Eurojust y Europol a las jurisdicciones involucradas, traspaso que se cumplió con todas las garantías reconocidas en la normativa y permitió el arresto de 10 traficantes. BURUIANA DANIELA, Miembro Nacional de Rumanía en Eurojust, se expresaba en los siguientes términos: *"I am delighted that Eurojust has been able to provide swift and professional support to this investigation and contribute to the success of taking down this criminal network. Without the timely, professional, and coordinated intervention of the competent national authorities involved in this operation, the drugs would have reached the market and created serious consequences for people's lives[109]"*.

La Agencia Eurojust, a falta de decisión de adecuación por parte de la Comisión Europea para poder transferir datos a un Estado no miembro directamente, ha suscrito acuerdos con un total de 12 terceros países: Albania, Montenegro, Macedonia del Norte, Serbia, Georgia, Islandia, Liechtenstein, Moldavia, Noruega, Suiza, Ucrania y Estados Unidos[110]. Estos acuerdos, en resumen, recogen los pasos a seguir para una transferencia recíproca entre el Estado en cuestión y Eurojust mediante el empleo de un *Liaison Prosecutor* nombrado por el primero y destinado en la sede del segundo. Además, estos mismos acuerdos

[108] Vid. el Considerando 71 de la Directiva (UE) 2016/680: *"el responsable del tratamiento puede tener en cuenta los acuerdos de cooperación celebrados entre Europol o Eurojust y terceros países que permitan el intercambio de datos personales al llevar a cabo la evaluación de todas las circunstancias que concurran en la transferencia de datos".*

[109] Document 2022/00071 adopted on 11th April 2022 by Eurojust. *10 arrests following a controlled delivery of drugs across Europe.*

[110] Aunque en el caso de Suiza se trata de un acuerdo a posteriori por cuanto la Comisión Europea mediante Decisión 2000/518/CE de 26 de julio de 2000 ya determinó que Suiza tenía un nivel adecuado de protección.

reconocen una serie de garantías de seguridad que habrán de cumplir las partes, así como la corrección y supresión de los datos en caso necesario[111].

El Consejo de la Unión Europea, por su parte, se ha pronunciado en resolución 13943/21, de 18 de noviembre, en relación con el impacto que tuvo desde su entrada en vigor la directiva objeto de trasposición. Sus conclusiones no merecen mayor explicación: *"[…] the introduction of the Directive has had and continues to have a significant impact on awareness and has further increased the security of the data processing among competent authorities, in particular among judicial and police authorities".* De igual manera, el Consejo incide en la importancia de la cooperación de los Estados miembros entre sí, así como respecto de las nuevas tecnologías para reforzar la normativa y la capacidad de las autoridades competentes en la consecución de los fines pretendidos por la directiva. Así, en estas mismas conclusiones, el Consejo se pronuncia con las siguientes palabras: "*the Council encourages the Commission and the Member States to invest more to consolidate expertise and knowledge and provision of human resources to help implementing The Directive in the daily operations of the competent judicial and police authorities. In that regard, particular attention should be given to the meetings organised through EDEN (European Data Protection Expert Network), on the dissemination of good practices and the exchange of views on data protection issues".* La anterior resolución del Consejo se adoptó con el objetivo de dotar a la Comisión del *feedback* necesario para la elaboración del informe que, según el artículo 62 de la Directiva (UE) 2016/680, debe presentar a más tardar el 6 de mayo de 2022[112].

Visto todo lo anterior, concluimos irrefutablemente que la reforma de la Directiva (UE) 2016/680 ha cumplido con lo que preveía el factsheet al que hacíamos

[111] Vid. a efectos meramente ilustrativos, el Cooperation Agreement between Eurojust and Switzerland adopted on 27th November 2008, artículos 10 y ss. El resto de acuerdos tienen una estructura prácticamente similar y no compete hablar de cada uno de ellos separadamente.

[112] Según este precepto, la Comisión europea, garante del correcto cumplimiento de los tratados y del derecho comunitario, tiene la obligación de presentar una evaluación del impacto que tuvo la entrada en vigor de la Directiva (UE) 2016/680 a fecha 6 de mayo de 2022, y posteriormente cada cuatro años. No es extraño que la publicación de esta evaluación se haya demorado en el tiempo estando prevista su finalización para finales de junio de 2022 debido al complejo procedimiento de elaboración al que ha sido sometido. Tanto el Parlamento como el Consejo han presentado sus propias conclusiones al igual que los propios ciudadanos quienes han tenido la oportunidad de expresar sus opiniones mediante la página web de la Comisión europea. Desafortunadamente, estamos en espera del informe final que deberá presentar la Comisión al Parlamento europeo y al Consejo.

referencia anteriormente, evitando la materialización de ciertos delitos que, de haberse producido, podrían haber causado el perjuicio de decenas, quizá cientos, de personas. Ahora bien, como ciertamente justifica BLASI CASAGRAN *"aunque la Directiva supone un progreso considerable en cuanto a las normas de protección de datos en comparación con la anterior Decisión Marco, sigue existiendo una fragmentación de normas en este ámbito. Muchos sistemas de la información en la Unión Europea quedan excluidos del ámbito de aplicación de la Directiva*[113]*"*.

Casualmente, los próximos días 16 y 17 de junio de 2022, el Supervisor Europeo de Protección de Datos celebrará una conferencia sobre el futuro de la protección de datos dentro del marco de la *EDPS Strategy 2020-2024* con el título *"the future of Data Protection: effective enforcement in the digital world"*. Según el *leaflet* de la conferencia: *"the first years of the GDPR's operation revealed much progress in the way personal data is protected across the digital domain. However, some shortcomings were also brought to light […] the conference will seek to explore both constructive improvements that exist within the current framework, but also alternative models of enforcement of the GDPR, including a more centralised approach*[114]*".* De hecho, el día 8 de diciembre de 2021 la Comisión europea presentó un proyecto denominado *"Código de cooperación policial de la Unión Europea"* que incluiría una propuesta de Reglamento relativo al intercambio automatizado de datos para la cooperación policial, por el que se modifican las Decisiones 2008/615/JAI y 2008/616/JAI del Consejo y los Reglamentos (UE) 2018/1726, 2019/817 y 2019/818; y una propuesta de Recomendación del Consejo relativa a la cooperación policial operativa. Los objetivos de este código de cooperación policial sería el de *"garantizar que las autoridades policiales de cualquier Estado miembro disfruten de un acceso equivalente a la información disponible en otros Estados miembros con el fin de prevenir y detectar infracciones penales y llevar a cabo investigaciones u operaciones contra la delincuencia, de modo que se superen las normas nacionales actuales, que impiden que la información fluya de forma eficaz y eficiente".* La normativa actualmente vigente, hemos visto, facilita enormemente el intercambio de datos

[113] Vid. BLASI CASAGRAN, en TRONCOSO, REIGADA, A. (Dir.), 2021: pág. 347.
[114] *Leaflet on the future of data protection: effective enforcement in the digital world by the European Data Protection Supervisor.*

e información entre Estados miembros, aunque atendiendo a esta propuesta normativa de la Comisión, cuando se habla de la fluidez de la información de forma eficaz y eficiente, entendemos se refiere a un acceso inmediato o directo a la información policial de otros estados mediante el sistema de ventanilla única. Sin duda esta pretensión normativa supondría un gran paso en el desarrollo de la cooperación policial, aunque su contenido y alcance no han quedado del todo delimitados. Como concluye WOJCIECH WIEWIÓROWSKI, actual Supervisor Europeo de Protección de Datos: *"los considerandos deberían explicar con mayor claridad la relación con el marco jurídico actual en materia de protección de datos. Además, la propuesta debería abstenerse de hacer referencia al RGPD, […] debería definir claramente el ámbito de aplicación personal de los intercambios de información previstos y limitar las categorías de datos personales que pueden intercambiarse sobre los testigos y las víctimas, en consonancia con el artículo 6 de la Directiva 2016/680 y con el enfoque adoptado en el anexo II del Reglamento (UE) relativo a Europol*[115]*".*

Como nos ha demostrado desde su fundación la Unión Europea, hace ya más de 70 años, el Derecho Comunitario está en constante evolución y cada vez alberga una importancia mayor para los Estados miembros. Esta normativa no es más que un pequeño paso más en el objetivo de la integración plena europea, ideal de la Unión desde la Declaración Schuman en mayo de 1950, pero no tengamos ninguna duda de que el arrollador avance tecnológico hará necesario un nuevo marco jurídico comunitario que sea de aplicación directa en los Estados miembros para hacer frente conjuntamente a los desafíos y retos que nos deparará en unas pocas décadas la Era Post-Digital.

IX. Bibliografía

Manuales y monografías

ARANGÜENA FANEGO, Coral y DE HOYOS SANCHO, Montserrat (2018). *Garantías procesales de investigados y acusados: situación actual en el ámbito de la Unión Europea.* Valencia. Tirant lo Blanch.

[115] Por todo el párrafo, según el resumen del dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de una Directiva relativa al intercambio de información entre las autoridades policiales de los Estados miembros, en Diario Oficial de la Unión Europea 2022/C154/05, de 8 de abril.

BERROCAL LANZAROT, Isabel (2017). *Derecho de supresión de datos o derecho al olvido.* Madrid. Reus.

DE TERWANGNE, Cécile (2012). *Privacidad en internet y el derecho a ser olvidado/derecho al olvido.* Revista d'Internet, dret i política, Nº13, 53-56.

DESGENS-PASANAU, Guillaume (2016). *La protection des données personnelles.* Paris. LexisNexis.

DI PIZZO CHIACCHIO, Adrián (2018). *La expansión del derecho al olvido digital: efectos de "Google Spain" y el Big Data e implicaciones del nuevo Reglamento Europeo de Protección de Datos.* Barcelona. Atelier.

DÍAZ ALABART, Silvia (2020). *La protección de los datos y contenidos digitales de las personas fallecidas.* Madrid. Reus.

HERRÁN ORTIZ, Ana Isabel (1998). *La violación de la intimidad en la protección de datos personales*. Madrid. Dykinson.

LÓPEZ ÁLVAREZ, Luis Felipe (2017). *Protección de datos personales: adaptaciones necesarias al nuevo reglamento europeo.* Madrid. Francis Lefebvre.

LÓPEZ GUERRA, Luis, ESPÍN TEMPLADO, Eduardo y VV.AA. (2018). *Derecho Constitucional. Volumen I. El ordenamiento constitucional. Derechos y deberes de los ciudadanos.* Valencia. Tirant lo Blanch.

RALLO LOMBARTE, Artemi (2019). *Tratado de protección de datos: actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.* Valencia. Tirant lo Blanch.

SÁNCHEZ DOMINGO, María Belén (2017). *La protección de datos personales en el espacio de libertad, seguridad y justicia. Especial consideración a las transferencias de datos a terceros países y organizaciones internacionales según la Directiva 2016/680.* Revista de Estudios Europeos, Nº69, enero-junio, págs. 17-36.

SÁNCHEZ GONZÁLEZ, Santiago (2003). *De la imponderable ponderación y otras artes del Tribunal Constitucional.* Revista Teoría y Realidad Constitucional, Nº12/13, 351-382.

TRONCOSO REIGADA, Antonio (2021). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales Volumen I y II.* Cizur Menor: Aranzadi.

VALLS PRIETO, Javier (2017). *Problemas jurídico penales asociados a las nuevas técnicas de prevención y persecución del crimen mediante inteligencia artificial.* Madrid. Dykinson.

Los artículos de revista que se incluyen como bibliografía han sido extraídos de la página web https://dialnet.unirioja.es/

Jurisprudencia y legislación

Código Civil.

Constitución española de 1978.

Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008 , relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

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 respeta al tratamiento de datos personales y a la libre circulación de estos datos.

Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y comunicación en la Administración de Justicia.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Ley 50/1981, de 30 de diciembre, por el que se regula el Estatuto Orgánico del Ministerio Fiscal.

Ley de Enjuiciamiento Civil.

Ley de Enjuiciamiento Criminal.

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales.

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales.

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Llei 10/2017, de 24 de juny, de les voluntats digitals i de modificación dels llibres segon i quart del Codi civil de Catalunya.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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.

STC 207/1996, de 16 de diciembre.

STC 292/2000, de 30 de enero.

STC 31/1981, de 28 de julio.

STC 53/1985, de 11 de abril.

STC 7/2019, de 17 de enero.

STJUE de 13 de mayo de 2014, asunto Google Spain, C-131/12.

STJUE de 16 de julio de 2020, asunto Facebook Ireland y Schrems, C-311/18.

STJUE de 17 de julio de 2014, asunto YS, C-141/12.

STJUE de 19 de octubre de 2016, asunto Breyer, C-582/14.

STJUE de 24 de noviembre de 2011, asunto Scarlet Extended, C-70/10.

STJUE de 25 de febrero de 2021, asunto Comisión Europea v. Reino de España, C-658/19.

STJUE de 30 de mayo de 2013, asunto Worten, C-342/12.

STJUE de 6 de octubre de 2015, asunto Schrems, C-362/14.

STJUE de 7 de mayo de 2009, asunto Rijkeboer, C-553/07.

Resoluciones y publicaciones de Autoridades.

Cooperation Agreement between Eurojust and Switzerland adopted on 27th November 2008.

Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.

Dictamen 3/2013, de 2 de abril, del Grupo de Trabajo del Artículo 29 (Documento WP 203).

Dictamen 6/2014, de 9 de abril, del Grupo de Trabajo del Artículo 29 (Documento WP 217).

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de una Directiva relativa al intercambio de información entre las autoridades policiales de los Estados miembros, en Diario Oficial de la Unión Europea 2022/C154/05, de 8 de abril.

Document 2022/00071 adopted on 11th April 2022 by Eurojust. *10 arrests following a controlled delivery of drugs across Europe.*

Eurojust's Annual Report 2020.

Factsheet of the European Commission adopted in January 2016, *how will the Data Protection reform help fight international crime?*

Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al Reglamento General de Protección de Datos. Agencia Española de Protección de Datos. Madrid. 2018.

Guidelines 4/2019 on article 25 Data Protection by design and by default adopted on 20th October by the European Data Protection Board.

Informe 0065/2015, de 9 de marzo de 2016 de la Agencia Española de Protección de Datos.

Informe 327/2003, de 25 de septiembre, de la Agencia Española de Protección de Datos.

Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos.

Leaflet on the future of data protection: effective enforcement in the digital world by the European Data Protection Supervisor.

Opinion 5/2018, adopted on 31st May on Preliminary Opinion on privacy by design by the European Data Protection Supervisor.

Resolución 13943/21, de 18 de noviembre de 2021, sobre la posición y conclusiones del Consejo sobre la aplicación de la Directiva (UE) 2016/680.

WP12 – Documento de trabajo sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de la UE sobre protección de datos, adoptada el 24 de julio de 1998 por el Grupo de Trabajo del Artículo 29.

Webgrafía

https://dialnet.unirioja.es/

https://edpb.europa.eu/edpb_en

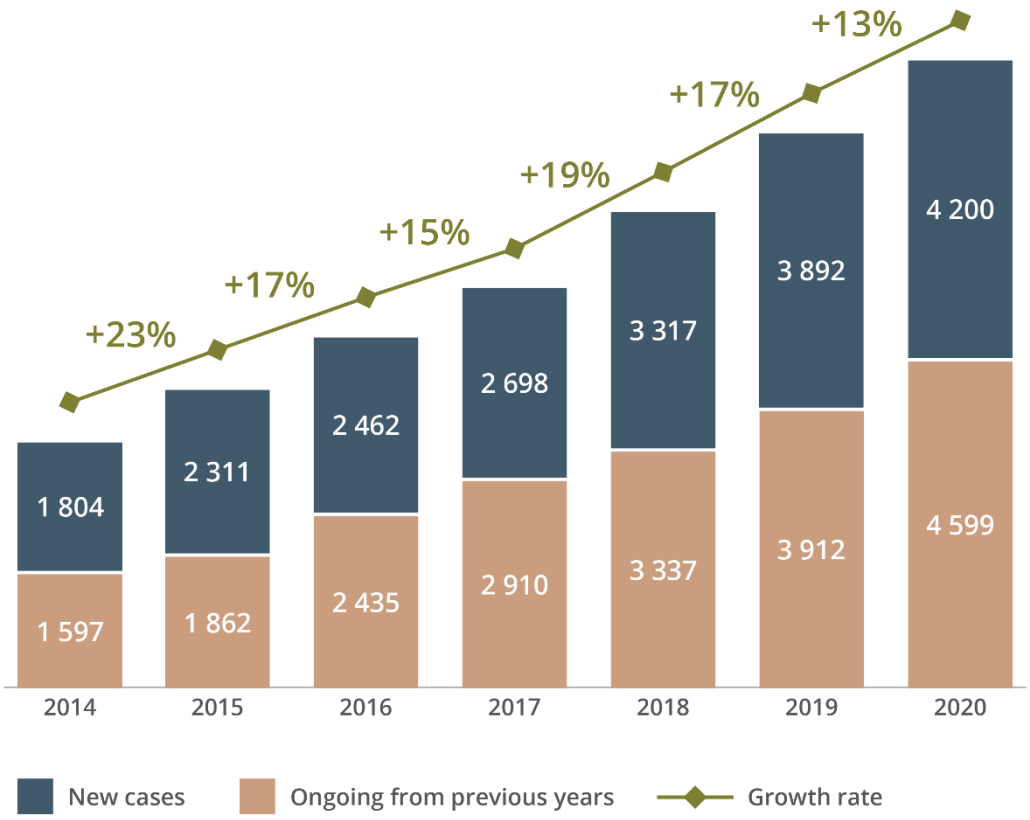
https://edps.europa.eu/_en

https://www.aepd.es/es

https://www.eurojust.europa.eu/

https://www.europol.europa.eu/

X. Anexo



El gráfico se ha extraído de la página oficial de Eurojust arriba mencionada.