THE EXTERNALISATION OF EUROPE’S DATA PROTECTION LAW IN MOROCCO: AN IMPERATIVE MEANS FOR THE MANAGEMENT OF MIGRATION FLOWS

Francesca TASSINARI

ABSTRACT: EU data protection Law allows the transfer of personal data to third countries and international organisations only when the European protection standards are met. This condition demands for the externalisation of the EU legal framework to ensure the flow of information in all sectors. Morocco has been moving towards the EU data protection principles for trade purposes, tough it has not reached an equivalent level of protection as required by Article 44 General Data Protection Regulation (GDPR). As a result, the exchange of personal data from the EU to Morocco is based on less guarantors means as far as the individuals’ fundamental rights are concerned. Concretely, the operational activity conducted by the European Border and Coast Guard to return irregular migrants is founded on the derogative clause of «important reasons of public interest». This article maintains that the approximation of Moroccan law to the continental one is an indispensable means to fairly manage migration flows. For this purpose, the EU not only promotes high data protection standards, but it also outsources its IT model enclosed in the Interoperability Regulations, no. 817 and 818 of 2019.

KEY WORDS: International data transfer, General Data Protection Regulation (GDPR), Morocco, Migrants management, Interoperability of AFSJ large-scale IT systems.

1 PhD Researcher, University of Granada, Spain. Researcher ID: H-5751-2018, ORCID ID: 0000-0003-4487-7130. This work was originally a contribution to the International Conference organised by the Jean Monnet Centre of Excellence «Migration and Human Rights in Europe’s External Borders», held in Tangier (Morocco), on November, 28th and 29th 2019. Special thanks shall be addressed to Prof. Del Valle Gálvez and Prof. El Houdaïgui, as well as to Prof. Fajardo del Castillo for her insightful suggestions. Any errors remain at my expense.
The Externalization of Europe’s Data Protection Law in Morocco: an Imperative Means for the Management of Migration Flows


MOTS-CLÉS: Transfert international de données, Règlement général sur la protection des données (RGPD), Maroc, Gestion des migrants, Interopérabilité des systèmes IT à grande échelle de l’ELSJ.

LA EXTERNALIZACIÓN DE LA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS EN MARRUECOS: UNA MEDIDA INDISPENSABLE PARA LA GESTIÓN DE LOS FLUJOS MIGRATORIOS

RESUMEN: La ley de protección de datos de la UE sólo permite la transferencia de datos personales a terceros países y organizaciones internacionales cuando se cumplen las normas de protección europeas. Esta condición exige la externalización del marco jurídico de la UE para garantizar el flujo de información en todos los sectores. Marruecos se ha acercado a los principios de protección de datos de la UE para fines comerciales, pero no ha alcanzado un nivel de protección equivalente al exigido por el artículo 44 del Reglamento General de Protección de Datos (RGPD). En consecuencia, el intercambio de datos personales de la UE a Marruecos se basa en medios menos garantistas en lo que respecta a los derechos fundamentales de las personas. Concretamente, la actividad operativa llevada a cabo por la Guardia Europea de Fronteras y Costas para devolver a los migrantes irregulares se basa en la cláusula derogatoria de «importantes razones de interés público». Este artículo sostiene que la aproximación del derecho marroquí al continental es un medio indispensable para gestionar de forma justa los flujos migratorios. Para ello, la UE no sólo promueve altos estándares de protección de datos, sino que también externaliza su modelo informático encerrado en los Reglamentos sobre la Interoperabilidad, n° 817 y 818 de 2019.

PALABRAS CLAVE: Transferencia internacional de datos, Reglamento General de Protección de Datos (RGPD), Marruecos, Gestión de migrantes, Interoperabilidad de sistemas TI a gran escala del ELSJ.
I. INTRODUCTION

This Note tries to consider the crucial role played by the exchange of information for the management of migration flows, with particular emphasis on the EU-Morocco relationship. In order to demonstrate the existing interrelation between the European Union (hereinafter EU) data protection policy and the migration one, the analyses below is organised as follows: firstly, it introduces the EU competence on personal data and the regime allowing its exchange with third countries; secondly, it gives an introspection on the EU-Morocco trade relationship and its impact on the management of migration flows and, finally, it shows how the transfer of personal data between the EU and Morocco is mainly conducted at the operational level thanks to the implementation of interoperable large-scale IT systems and the brokering of EU agencies, taking as an example the European Board and Coast Guard agency’s (hereinafter EBCG Agency) activity for the return of irregular migrants.

II. THE INTERNATIONAL TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES: AN EU APPROACH

As long as global standards do not exist, diversity will remain. Transborder data flows have to be facilitated whilst, at the same time, ensuring a high level of protection of personal data when they are transferred to and processed in third countries.2

Global standards on the protection of personal data are indispensable to guarantee the flow of information worldwide.3 The EU has been committed to the protection of personal data of its citizens and residents from the very beginning of the technological revolution.4 Today, the EU has become one of the most important players to actively promote the fundamental rights to

---


privacy and to the protection of personal data thanks to its peculiar recognition in EU primary law.⁵

1. The EU Competence on the Protection of Personal Data and its Free Movement

During the 1970s, the rapid evolution of information technology (IT) enabled the automatic processing of huge amount of personal data by European companies raising the concerns of the international community on the respect of the fundamental right to a private and family life.⁶ A first regional harmonisation was laid down by the Council of Europe in the Convention no. 108 for the protection of people against the automated processing of personal data.⁷ The Treaty served as a starting point for the EU when developing its own legal framework in 1995, namely Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data (Data Protection Directive hereinafter).⁸ The European Community and bodies were firstly bound by the

---


⁷ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS n° 108, 28.01.1981, and its relevant Protocols: Additional Protocol for the Protection of Individuals with regard to Automatic Processing of Personal Data to the Supervisory Authorities and cross-border data flows of 8 November 2001, ETS n° 181 (ratified by forty-four parties among which eight countries that are not part of the Council of Europe, last consult on 21st March 2021), and Additional Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 10 October 2018, ETS n° 223 (it counts on eleven ratification among which one country is not part of the Council of Europe, last consult on 21st March 2021). On the leading role played by the continental data protection model see, for example, Greenleaf, G., “The influence of European data privacy standards outside Europe: implications for globalization of Convention 108”, International Data Privacy Law, Vol. 2, n° 2, May 2012, pp. 68–92. DOI: https://doi.org/10.1093/idpl/ips006.

⁸ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free
data protection principles under Article 286 TEC of the Amsterdam Treaty in 1997. This disposition was substituted by current Article 16 TFEU that empowers the European Parliament and the Council to adopt rules relating to the protection of individuals «[…] with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data». Article 16(2) TFEU provides the EU with a horizontal-concurrent competence that acquires sectoral application in certain areas or under pre-defined EU policies. Besides, the Treaty of Nice entrenched data protection in a specific provision on the fundamental right to the protection of personal data that is now recognised in the EU Charter of Fundamental Rights independently from the right to a private and family life. movement of such data (OJ L 281, 23.11.1995, p. 31–50).

9 According to which: «From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty», Treaty establishing the European Community (Consolidated version 1997) (OJ C 340, 10.11.1997, pp. 173–306).


13 Article 7: «Everyone has the right to respect for his or her private and family life, home and communications; and Article 8: «1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority», in Charter of Fundamental Rights of the European Union (OJ C 326, 26.10.2012, p. 391–407). Some hints on the distinction between Article 8 of the Charter and Article 8 of the European Convention on Human Rights of 4 November 1950 are made by RODOTA, S., “Data Protection as a Fundamental Right”, in Gutwirth, S., et al., Reinventing Data Protection?, Springer, The Netherlands. 2009, pp. 77-82, as well as by KOKOTT, J., and SOBOTT, C., “The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR”, International Data Privacy Law, Vol. 3, n° 4, November 2013, pp. 222–228. DOI: https://doi.org/10.1093/idpl/ipt017. On their convergence, instead, see
2. The EU Regime on the International Transfer of Personal Data

Under the new General Data Protection Regulation (hereunder GDPR) international data transfer is governed by the main principle set forth in Article 44 for which the disclosure of personal data to third parties shall not undermine the level of protection guaranteed under that Regulation. Otherwise, personal data destined to or contained in the European files cannot be exchanged. This prohibition has crucial impacts on EU external policies, especially international trade ones, since it may hamper the economy of both the EU and the third country or organisation. To avoid any damage, the EU promotes continental data protection standards beyond its borders, concretely, the transfer of


For example, with the dissemination of democratic principles under the South III Program together with the Council of Europe. The information is available in the official website of the latter here: http://southprogramme3-eu.coe.int.

personal data from the EU to foreign countries and international organisations is regulated under three alternative forms: adequacy decisions, appropriate safeguards, and derogation clauses. Adequacy decisions represent the most guaranteeing instrument since they allow a global evaluation of the foreign legal system and have direct effect in the Member States’ legal orders. In this sense, adequacy decisions only enable the information to fluently flow beyond the EU external borders.

III. EU-MOROCCO TRADE RELATIONS: THE WAY FORWARD TO EXTERNALISE DATA PROTECTION PRINCIPLES

2019 has been a positive year for Morocco that reaffirmed its position as a strategic partner of the EU external relations. Thanks to its colonial ties, Morocco has always benefited from a favourable treatment in terms of market conditions. Already the Rome Treaty ensured Morocco more advantageous

20 Article 45 GDPR.
21 Article 46(2) and (3) GDPR.
customs procedure,\textsuperscript{25} and the six founding States committed to build up an EU-Morocco economic association.\textsuperscript{26}

Following the Barcelona Process, the Euro-Mediterranean Partnership Agreement concluded between the EU and Morocco in 1996 marked a turning point for the establishment of an advanced status of Morocco. Indeed, the intergovernmental dialogue included the enhancement of relationships on several fronts: political; economical; financial; social, and cultural.\textsuperscript{27} On that occasion, the EU promoted its basic values and fundamental principles inserting a democratic clause comprising the protection of human rights,\textsuperscript{28} including a list of data protection principles applicable to the EU-Morocco trade relations.\textsuperscript{29} These principles basically retraced the Data Protection Directive, a European standard that Morocco accepted in its domestic law by

\textsuperscript{25} Treaty establishing the European Community (consolidated version) - D. Protocols annexed to the Treaty establishing the European Community - Protocol n° 13 on goods originating in and coming from certain countries and enjoying special treatment when imported into a Member State (1957) (\textit{OJ} C 321 E, 29.12.2006, p. 250).


\textsuperscript{29} Euro-Mediterranean Agreement establishing an association between the European Communities and their Member States, of the one part, and the Kingdom of Morocco, of the other part - Protocol 1 on the arrangements applying to imports into the Community of agricultural products originating in Morocco - Protocol 2 on the arrangements applying to imports into the Community of fishery products originating in Morocco - Protocol 3 on the arrangements applying to imports into Morocco of agricultural products originating in the Community - Protocol 4 concerning the definition of originating products and methods of administrative cooperation - Protocol 5 on mutual assistance in customs matters between the administrative authorities - Final Act - Joint Declarations - Agreements in the form of an Exchange of Letters - Declaration by the Community - Declarations by Morocco (\textit{OJ} L 70, 18.3.2000, p. 2–204).
adopting Law 09-08. Despite this, in 2010 the Moroccan Law did not pass the adequacy test of the European Commission that would have enabled the free flow of data by virtue of Article 36 Data Protection Directive. All in all, the Moroccan divergent regulation remits to an underlying legal system built upon its own set of principles and values. Law 09-08, for example, echoes Muslim religion by not including sexual life and sexual orientation within the definition of sensitive data, in contrast to the GDPR.

In the EU-Morocco Action Plan (2013-2017) both parties committed to realise «an area of shared values» in which Morocco particularly would have made further efforts to «raise awareness among all parties and stakeholders concerned at national level of the importance of following the principles and values laid down by the Council of Europe’s European Convention on Human Rights, the EU Charter of Fundamental Rights, the Partial Agreements of

30 Dahir No. 1.09.15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi N°. 09-08 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel, BO n° 5714 - 7 rabii I 1430 (5.3.2009). Available at: https://www.cndp.ma/images/lois/Loi-09-08-Fr.pdf. Last consult on 26th April 2021.


33 Article 3(1) Law 09-08: «Données sensibles: données à caractère personnel qui révèlent l’origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l’appartenance syndicale de la personne concernée ou qui sont relatives à sa santé y compris ses données génétiques».

34 Article 9(1) GDPR: «Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited». Generally, on the adequacy of African countries see BONIFACE MAKULILLO, A., “Data Protection Regimes in Africa: too far from the European ‘adequacy’ standard?”, International Data Privacy Law, 2013, Vol. 3, n° 1, pp. 42-50.
the Council of Europe, and the relevant EU directives [...]».\textsuperscript{35} Morocco was strongly encouraged to adopt the European model and especially to adhere to the Council of Europe Convention no. 108, which it finally did in January 2019.\textsuperscript{36}

In the meantime, The Data Protection Directive was reappealed by the new GDPR in force since May 2018, the 25\textsuperscript{th}. While maintaining the international data transfer model of the Data Protection Directive, the GDPR introduces significant changes that spur the flow of information between the EU and third countries and international organizations. Specifically, the GDPR: 1. establishes new instruments for legitimising international data transfers that are spread on three different layers — namely adequacy decisions\textsuperscript{37}, appropriate safeguards,\textsuperscript{38} and derogative clauses,\textsuperscript{39} and 2. it suppresses bureaucratic requirements that hindered international trades and, concretely, the need of a specific authorisation in the absence of an adequacy decision, as well as the duty of data controllers or processors to notify the supervisory authority of any wholly or partly automatic processing operation or set of such operations.\textsuperscript{40} In any case, adequacy decisions remain the primary preferable channel to transfer personal data since this instrument calls for the European Commission to realise an in-depth analysis of the third party’s legal order and international commitments, including the respect of Rule of Law and Fundamental Rights’

\textsuperscript{35} Council Decision of 21 October 2010 on the position to be taken by the European Union within the Association Council set up by the Euro-Mediterranean Agreement establishing an association between the European Communities and their Member States, of the one part, and the Kingdom of Morocco, of the other part, with regard to the adoption of provisions on the coordination of social security systems (2010/697/EU) (OJ L 306, 23.11.2010, p. 1–1).

\textsuperscript{36} Precisely, it ratified it on 01.01.2019, Member States’ signatures and ratifications are available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?pauth=72dZxGWV, Last consult on 26 April 2021.

\textsuperscript{37} Article 45 GDPR.

\textsuperscript{38} Article 46 GDPR.

\textsuperscript{39} Article 49 GDPR.

\textsuperscript{40} In the Spanish case, for example, the Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, BOE n° 298, de 14.12.1999, required data experts to ask for the Agencia Europea de Protección de Datos (AEPD) a prior authorization to transfer data to importers established in third countries that did not have an adequate level of protection, as long as they provided certain guarantees. In case they did have this level, then, a notification was sufficient – see Article 33.

All things considered, moving towards the European parameters Morocco would gain the issuance of an adequacy decision which would enhance a fast-track proceeding exchange of personal data. By doing so, the two partners would kill two birds with one stone: on one hand, Morocco would ensure its privileged access to the European Single Market; on the other one, the EU-Morocco alliance would open up safe and effective commercial channels to their operators.

IV. 2.0 MANAGEMENT OF MIGRATORY FLOWS

The exchange of information has acquired a leading role in the management of the EU migration policy, especially to overcome the lack of collaboration by third countries of transit and origin. Nevertheless, the disclosure of personal data to third parties raises concern with regard to the protection of individuals’ fundamental rights and, specifically, the right to privacy and the right to the protection of personal data. A regulatory convergence of

---

41 Article 45(2) GDPR.

42 See the list of countries with which a decision in this regard has already been taken in: https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html. Last consult on 29th April 2021.

43 The innovation of the EU trade policy under the aegis of new technologies has been clearly affirmed by the European Commission in its Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Trade Policy Review - An Open, Sustainable and Assertive Trade Policy, COM(2021) 66 final, Brussels, 18.2.2021. Notably, on the issue of data it states that: «The Commission will work towards ensuring that its businesses can benefit from the international free flow of data in full compliance with EU data protection rules and other public policy objectives, including public security and public order. In particular, the EU will continue to address unjustified obstacles to data flows while preserving its regulatory autonomy in the area of data protection and privacy», at p. 15.

44 Inspired by the brilliant reflections made by the relevant doctrine in DE BRUYCKER, P., DE SOMER, M., and DE BROUWER, J. L., “From Tampere 20 to Tampere 2.0: Towards a new European consensus on migration”, European Policy Centre, 2019.

Morocco standards in the protection of personal data will unavoidably impact the management of migratory flows from and toward the EU as it is further explored below.

1. An Unattractive EU Migration Policy: The Morocco Case

While EU-Morocco trade relations have been progressively deepening with satisfactory results, their migration policies strongly diverge due to the subsistence of different perceptions and priorities. The negotiations for an EU-Morocco readmission Agreement that started in 2000 have never seen the light. Likewise, the implementation of the mobility agreement signed in 2013 has been cyclically suspended because of further strains, such as the difficult negotiation of an agricultural and fisheries Treaty. One of the most critical points of the negotiations pivoted around the return of third country nationals who attempt to irregularly enter or stay in the territory of a Member State. In a nutshell, Morocco refuses to accept third countries nationals because its commitment goes to the management of immigration flows from the southern Sahara and, even more importantly, because it fears to becoming a buffer State by welcoming thousands of third-country nationals. On the contrary, Morocco accepts the readmission of its own nationals subject to the granting of huge economic benefits and greater flexibility as far as the EU visa policy is concerned.

2. The Role of Large-Scale IT Systems and their Interoperability in the Management of Migratory Flows

The wide spreading of improved and cheaper biometric technology is increasingly supporting global policies directed to the management of external

48 Joint Declaration Establishing A Mobility Partnership Between The Kingdom Of Morocco And The European Union And Its Member States, Brussels, 3 June 2013 (05.06), 6139/13 Add1rev3.
borders, migration flows,\textsuperscript{50} and security threats also, but not only, because of the development of long-distant recognition techniques.\textsuperscript{51}

A. Few Hints on Large-Scale IT Systems and their Interoperability

The EU commitment in the fields of smart borders and interoperability goes precisely in this direction. Concretely, the Visa Information System (VIS),\textsuperscript{52} the European Dactyloscopy System (Eurodac System),\textsuperscript{53} and the Schengen Information System (SIS II)\textsuperscript{54} have been recently reformed, while

\textsuperscript{50} Modi, S. K., \textit{Biometrics identity management concepts}, Edit. Artech House, Boston, 2011. It shall be noted that the Global Compact for Safe, Orderly and Regular Migration adopted on 11 December 2018 and lately formalised by the UN General Assembly in the A/RES/73/195, contemplates as a first objective the collection and use of data in an accurate and disaggregated manner as a basis for evidence-based policies. For an exhaustively comment on the Global Compact see Fajardo del Castillo, T., “The Global Compact for safe, orderly and regular migration a Soft Law instrument for management of migration respecting human rights”, \textit{Paix et sécurité internationales: Journal of International Law and International Relations}, n° 8, 2020, pp. 51-94.


\textsuperscript{53} Regulation (EU) No. 604/2013 of the European Parliament and of the Council of 26 June 2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person (OJ L 180, 29.6.2013, p. 31–59). See also the Amended proposal for a Regulation of the European Parliament and of the Council on the establishment of ‘Eurodac’ for the comparison of biometric data for the effective application of Regulation (EU) XXX/XXX [Regulation on Asylum and Migration Management] and of Regulation (EU) XXX/XXX [Resettlement Regulation], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States’ law enforcement authorities and Europol for law enforcement purposes and amending Regulations (EU) 2018/1240 and (EU) 2019/818, COM/2020/614 final, currently under negotiations.

\textsuperscript{54} Regulation (EC) No. 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration


and on September 23rd, 2020, proposed a new Pact on Migration and Asylum that increasingly relies on Artificial Intelligence.

All these reforms are characterized by the following circumstances: an increased number and type of data stored therein, including biometrics with the sole exception of ETIAS; the normalisation of the storage timeline up to a five-year period – deadline corresponding to the SIS II alerts known as entry ban, and the provision of automated checks that enable the systems to query each other without the need of human intervention.

Interoperability Regulations nos. 817 and 818 of 2019 crown the innovation of an EU border management strategy that rely more and more on large-scale IT systems in order to: improve the efficiency of inspections at external borders; contribute to prevent and combat irregular immigration, and achieve a high level of security within the Schengen area. The IT wave brought by the Interoperability Regulations relies upon four main components, that is: the European Search Portal (ESP); the Multiple-Identity Detector (MID); the shared Biometric Matching Service (sBMS), and the Common Identity Repository (CIR). The complexity of the sister Regulations prevents a quick analysis of their content. It is here sufficient to point out that this reform


61 Recital (9) of the Interoperability Regulations.

owes its success to the flood of personal data that migrants give, more or less consciously, to the EU to cross its external borders. In terms of cross-border impact, Interoperability will expedite the exchange of data between Member States and, as a consequence, between them and third countries.

B. The Transfer of Personal Data in the Operational Layer

Special attention shall be given to the operational activity carried out by EU agencies involved in the management of migration flows, among which the European Border and Coast Guard Agency stands out (EBCG Agency hereinafter). Thanks to its strategic partnership with third countries of origin and transit, the EBCG Agency will be able to compare the information recorded in large-scale IT systems with the one stored by third countries. Nevertheless, being this comparison a «transfer of personal data» from the EU to Morocco in terms of the GDPR, this shall be backed up by an appropriate legal basis. For example, in the case of returning irregular migrants, and in

---


65 According to Kuner, the concept of international data transfer shall include «[…] personal data that are sent or made accessible across national borders, rather than based on a set definition». See Kuner, C., “Chapter V Transfer of Personal Data to Third Countries or International Organizations (Articles 44-50). Article 44. General principle for transfers”, in Kuner, C., et al., The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, USA, 2020, pp. 762-762.

66 On the EU policy for returning irregular migrants see Fajardo Del Castillo, T., “La
absence of an adequacy decision, before the impossibility to conclude an EU-Morocco readmission agreement the transfer of information to this third country could be backed up by Frontex’s administrative arrangements authorised by the competent national supervisory authority or, as a last resort, the derogative clause of «important reasons of public interest». At the current day, Frontex and Morocco bilateral meetings have not been formalised in a working agreement so that personal data can be transferred only under derogative conditions. Yet, the processing of personal data for «general


Article 49(1)(d) GDPR.


The Externalization of Europe’s Data Protection Law in Morocco: an Imperative Means for the Management of Migration Flows

Public interest enables the restrictions of data subjects’ subjective rights such as: the right to information, to access, rectify and erase personal data; the right to restrict the processing of personal data; the right to object the processing of personal data, and the right to not to be subject to a decision based solely on automated processing.¹³ For this reason, this clause shall be interpreted restrictively, as the ultima ratio justifying ad hoc exchange of personal data.¹⁴

Last but not least, the possibility that Morocco is the one transferring or disclosing personal data to the EU shall also be contemplated as far as data protection rules obstacle an efficient operational policy. Provided that Morocco is cooperative, neither Member States’ nor EU’s authorities can be considered «recipient» in terms of the GDPR and are subject to data protection (hereinunder Frontex Regulation), whose recital (101) states that:

In order to properly implement its tasks in the area of return, […] the Agency might need to transfer the personal data of returnees to third countries. The third countries of return are not often subject to adequacy decisions adopted by the Commission […] and have often not concluded or do not intend to conclude a readmission agreement with the Union or otherwise provide for appropriate safeguards […]. Where such agreements do not yet exist, personal data should be transferred by the Agency for the purposes of facilitating the return operations of the Union, provided that the conditions laid down in point (d) of Article 50 (1) of Regulation (EU) 2018/1725 are met.

¹³ Article 23(1)(e) GDPR. Notably, Article 86(3) of the Frontex Regulation specifies that the Agency shall indicate «[…] any restrictions on access to or use of those data, in general or specific terms, including as regards transfer, erasure or destruction. Where the need for such restrictions becomes apparent after the transfer of personal data, the Agency shall inform the third country or the international organisation accordingly».

¹⁴ Notably, the regime on international data transfer applicable to Frontex is the one regulated under Chapter V EUDPR, which excludes the application of the special dispositions so-called «operational data» set forth under Chapter IX. In Chapter IX, it is clearly maintained that the transfer can be backed up by an international agreement concluded between the EU and the third country – or international organization – pursuant to Article 218 TFEU «[…] adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals». However, this possibility leads back to the provision on appropriate safeguards and, concretely, to «legally binding and enforceable instrument between public authorities or bodies» set forth in Article 48(2)(a) EUDPR. Such an instrument can be concluded by the EU on the basis of Article 16 TFEU in application of the ATER doctrine or, most frequently, in a clause on data protection inserted in a treaty with a wider scope. On the EU external action see Liñán Nogueras, D. J., “La acción exterior de la Unión: las relaciones exteriores”, in Mangas Martín A. and Liñán Nogueras, D. J., Instituciones y derecho de la Unión Europea, Edit. Tecnos, Madrid, 2016, pp. 553-557.

¹⁵ Article 4(9) GDPR.
principles, for and for most, the principle of purpose limitation. Yet, the acceptance of personal data from a third country that does not comply with an adequacy decision may also hamper the exercise of data subject’s subjective rights, as the latter may not be guaranteed by the third state *tout court*. In this sense, and under the same rationale adopted in Title V GDPR, personal data should not be accepted from third States that do not meet the EU standard of protection. Despite this, the GDPR does not expressly address this issue and could have been more incisive to ensure the effectiveness of the protection granted under the EU roof.

Besides, the possibility to exchange personal data with third countries – specifically biometrics – requires a major effort from the EU, that goes beyond the externalisation of its data protection standards. Concretely, the EU shall outsource its biometric identity management model in foreign territories. An example is the case of Nigeria, a pioneer State in the implementation of digital database. Under the sponsorship of the International Organization for Migration (IOM), Nigeria now has a centralized database in Niamey that stores the data processed by the Migration Data Information and Analysis System (MIDAS), dedicated to the identification of travellers at the border entry and exit points.  

The system is connected to the US Personal Identification System for Safe Comparison and Evaluation (PISCES), the Interpol Alert System and the Eurosur system of the European Border and Coast Guard (EBCG). More recently, *Statewatch* has published last minute information on the EU funding for the implementation of biometric databases in Senegal.

V. CONCLUSION

The approximation of Morocco’s national law on the protection of personal data to the EU standards and values promoted in the commercial

---


77 Currently under reform, see “La Commission européenne précise les obligations de Frontex dans le cadre du système EUROSUR”, *Bulletin Quotidien Europe*, n° 12695, 10.4.2021.

field will have prominent impacts on the management of migration flows if it leads to the adoption of an adequacy decision. The latter is also the most guaranteeing solution from the perspective of the protection of migrants’ fundamental rights. The interoperability of large-scale IT systems provides efficient tools to smartly identify third country nationals which will facilitate the readmission of irregular migrants notwithstanding the conclusion of an EU-Morocco readmission agreement. This task is mainly deployed by the EU agencies and, concretely, the EBCG Agency that facilitates the transmission of personal data from the EU to third countries for the purposes of returning irregular migrants. While from an institutional point of view adequacy decisions require substantial reforms to guarantee the respect of individuals’ fundamental rights to privacy and to the protection of personal data, from an operational perspective the EU shall outsource its IT identification model in order to ensure its technical compatibility—which it has already started to do. A further field of study remains to be explored, namely the possibility that the implementation of the EU operational apparatus in third countries will allow the interconnection of foreign databases with the continental ones, including with the large-scale IT systems in the terms analysed above.

BIBLIOGRAPHICAL REFERENCES


KAISER, K., “EU-Morocco Negotiations on a Readmission Agreement: Obstacles to a Successful Conclusion”, *College of Europe EU diplomacy*, 2019.


WAGNER, J., “The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?”, *International Data Privacy Law*, Vol. 8, n° 4, 2018, pp. 318–337.