ISSN 2704-8012

European Journal of Privacy Law & Technologies



Special issue (2020)

G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

Special issue (2020)

Edited by Massimo Foglia

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in September 2020
www.ejplt.tatodpr.eu

GDPR – MAIN INTERNATIONAL IMPLICATIONS

Dulce Lopes, University of Coimbra

Abstract:

The General Data Protection Regulation aims to ensure a consistent and homogenous protection of data subjects rights throughout the territory of the European Union Member States and beyond. The broad scope and international reach of the GDPR is, therefore, a *hot topic,* that is currently under discussion and analysis both in Academia and in Courts. This article contributes to the subject, by examining the major international implications of the GDPR both in the private international law and in the international administrative law arenas, now widely conformed by European Union provisions and case law.

Keywords: Data Protection; Extraterritoriality; Data Transfers; Supervisory Authorities

Summary: 1. Introduction. – 2. GDPR extraterritorial effects: overview. – 3. Applicable rules on data protection. – 4. International data transfers. – 5. The supervisory mechanism. – 6. International civil and administrative procedural law. – 7. Conclusions.

1. Introduction

The protection of natural persons in relation to the processing of personal data is a fundamental right established, within the European Union, in Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). This protective aim is transversal to all European Union competencies and policies, even when implemented at a national level, which stands as, it should be added, the rule in the European Union judicial and administrative arenas.

However, this is not the only concern that lies behind Regulation (EU) 2016/679, enacted in 27 April 2016, by the European Parliament and the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and that repealed Directive 95/46/EC (General Data Protection Regulation, GDPR). It is clear from the debates previous to and the recitals of this Regulation that a robust entrepreneurial

reasoning is behind the need to stabilize a clear and coherent personal data protection framework that does not strongly differ from state to state. It is indeed the objective of ensuring "*an equivalent level of protection of natural persons and the free flow of personal data throughout the Union*" that is the basis of the necessary subsidiarity considerations within the GDPR (recital 170) [1].

Absent these considerations, it might have sufficed to maintain Directive 95/46/EC in force but with modifications [2] and with due implementation by Member States [3], and not going full force with a stronger legal harmonisation in this area. Despite this [4], the prevailing narrative is still fundamental rights protection, which is the main reason behind the broadening of the territorial scope of the GDPR and for its major international implications. Both issues constitute the objective of this article.

---

[1] There are two major exceptions or deviations to the application of the GDPR. It does not apply to "purely personal or household activity" [Article 2(1)(c)] such as for instance, establishing a mailing list with friends. Also, according to Article 30 (5), it only applies partially to organisations with fewer than 250 employees (small and medium sized enterprises).

[2] One of these modifications has to do with the new legal basis introduced by the Treaty of Lisbon (article 16 TFEU). No. 2 of this provision does not, however, impose any specific instrument (directive or regulation) in the field, just establishes a defined procedure (the ordinary legislative procedure). For instance, in criminal areas the option was for a Directive, given the sensitivities and national differences in the field [Directive (EU) 2016/680 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA]. For the main lines of review of the Directive, cf. P. HUSTINX, *EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation*, M. CREMONA (eds.), *New Technologies and EU Law* (Oxford 2017), 148-151.

[3] See for instance the judgment Case C- 275/06, Productores de Música de España (Promusicae) / Telefónica de España SAL, ECJ, 29.1.2008 that states that "[...] *Community law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality*".

[4] Discussing whether data protection should generally be seen as a fundamental right since it is more akin to market regulation than to traditional human rights instruments, cf. B. VAN DER SLOOT, *Legal Fundamentalism: Is Data Protection Really a Fundamental Right?*, R. LEENES ET AL. (eds.), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Berlin 2017), 3-30.

2. GDPR extraterritorial effects: overview

The protection of personal data faces new challenges. The exchange of personal data between private and public actors has increased widely, mostly due to online activities, paving the way to an unprecedented scale in collecting and sharing of personal data that might run contrary to the protection of fundamental rights.

The harmonized framework on data protection aims to ensure a consistent and homogenous application of the rules for the protection of data subject rights all throughout the territory of the European Union Member States and beyond.

Indeed, GDPR sets an unprecedented paradigm in which extraterritoriality is taken to its highest level. Even if Article 4 of Directive 95/46/EC had already established private international law rules on this issue that were seen as highly innovative – though rather troublesome [5] –, other instruments such as adequacy decisions played a relevant, but not undisputed, role in the EU's data protection framework. These issues are addressed in the GDPR. In addition, new mechanisms were introduced into the GDPR that constituted genuine novelties in this area.

Now administrative and jurisdictional issues related to the monitoring or infringements of data protection law tend to be regulated globally, in all its dimensions and layers. This has naturally reflexed in several areas of law that regulate international situations [6]: private international law (in particular conflict of laws), public international law, international administrative law and international civil (and administrative) procedural law. Let us look briefly at these implications in turn [7].

---

[5] I. REVOLIDIS, *Judicial Jurisdiction Over Internet Privacy Violations and The GDPR: A Case Of "Privacy Tourism"?* (2017) 11 (1) *Masaryk University Journal of Law and Technology*, 9-11; M. BRKAN, *Data Protection and Conflict-of-laws: A Challenging Relationship* (2016) 13 *European Data Protection Law Review,* 326.

[6] It should be mentioned that GDPR establishes, for certain purposes and mostly for administrative and judiciary implications, a distinction between international processing of data and a more defined concept of cross-bordering processing [Article 4 (23)] that includes only the processing of personal data that takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State and the processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

[7] This analysis will be made individually for explanatory purposes. However, the links between these areas of law are very close and intertwined. For instance, extraterritoriality in asserting jurisdiction and in applicable law should comply with basic public international law requirements and traditional public international law instruments such as agreements have been comple-

3. Applicable rules on data protection

The main concepts of GDPR that should be considered in what regards private international law rules inserted into the Regulation are the ones of the controller (the one that determines the processing of the data) and processor (the one that operates the data, whether or not by automated means). Simply put, if company A sells clothes in the European Union using company B, an emailing company to track and engage clients, the controller is company A and the processor company B.

On this account GDPR treats the data controller as the principal party for responsibilities such as collecting consent, managing consent-revoking, enabling right to access, etc. In addition, it introduces direct obligations for data processors that are subject to penalties and civil claims by data subjects and presented in a model that has already been named as a "cumulative" liability regime for controllers and processors [8].

That is why Article 28 (1) GDPR imposes upon the controller the choice of processors "providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject", such as approved codes of conduct, certified mechanisms and standard contractual clauses. However, there is no fixed line between a controller and a processor since if this determines the purposes and means of processing, the processor shall be considered to be a controller in respect to that processing [Article 28 (10)] [9].

These two entities are under specific obligations pursuant to Article 27 (1) of the GDPR since where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union [10], the controller or the processor should, in principle, designate a representative in the Union [Article 27 (1), recital 80]. This represents the introduction by the European Union of a specific

---

mented by other administrative and privative mechanism that allow for international transfer of data.

[8] B. VAN ALSENOY, *Liability under EU Data Protection Law - From Directive 95/46 to the General Data Protection Regulation* (2017) 7 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 282.

[9] This allocation of responsibilities incorporates the understanding under the Data Directive that processors can be joint controllers whenever they exert decisive influence over the phases of collection and transmission of data (cf., among others, the judgements Case C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, ECJ, 5.6.2018 and Case C-40/17, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, ECJ, 29.7.2019).

[10] And whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union.

private international law rule [already previewed in Article 4 (2) of the Directive] that requires a special substantive obligation for undertakings in international situations. It materialises the need for a "guarantor" located within the European Union in order to have a representative that should not only act on behalf of the controller or the processor but also be addressed by any supervisory authorities [11].

This requirement is in line with Article 3 of the GDPR, under the title "territorial scope". This rule establishes that "*This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not*" (1). Adding that "*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services* [12]*, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.*" (2) [13].

---

[11] Also, other obligations are envisaged, namely the necessary appointment of a (joint) data protection officer whenever the requirements of Article 37 (1) are met, which might extend to international controllers and processors not established in the European Union. This obligation might seem to be overreaching but taking into account that the DPO is an independent and concerned person that strengthens the monitoring and compliance of personal data protection, it forms a crucial part of the "division of responsibilities" laid down in the GDPR. Given its advisory position, the GDPR does not provide for rules on liability or sanctioning of the Data Protection Officer although this might be provided for in national legislations (cf. P. VOIGT-A. VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR) – a Practical Guide* (Berlin 2017), 61-62).

[12] This offering of goods and services should be read *cum granum salis.* We do not believe as P. DE HERT-M. CZERNIAWSKI, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context* (2016) 6 (3) *International Data Privacy Law*, 241, put it that the mere fact of having a website that is accessible in the European Union triggers this possibility (somewhat "*analogous to owning a bookshop*" for others to direct themselves to and browse). Indeed if a company is established outside the European Union and does not have any means of processing in the European Union, it should be considered that it falls under the GDPR if it is apparent (see Recital 23) that it offers through the internet goods and services in the European Union – for instance, by using local currencies such as the Euro, local languages or local top-level domains – and not only if it can be accessed by persons located in the European Union, which would be unreasonable (cf. https://gdpr.eu/companies-outside-of-europe/). These criteria are particularly needed since it is very difficult, if not nearly impossible, to insulate websites from "abroad visitors" (on this, see U. KOHL, *Jurisdiction and the Internet–Regulatory Competence over Online Activity* (Cambridge 2007), 278 ff.; and A. LOPÉZ-T. MARTÍNEZ, *El criterio de las actividades dirigidas como concepto autónomo de DIPR de la Unión Europea para la Regulación de las actividades en internet*, (2017) 69 (2) *Revista Española de Derecho Internacional,* 223-256). For non-exhaustive evidence from which it may be concluded that the activity is directed to persons in the European Union, see, although on another subject-matter, the judgment Joined Cases C-585/08 and C-144/09, Peter Pammer et al., ECJ, 7.12.2010, 93).

[13] Article 3(3) also determines that the Regulation applies to the processing of personal data

This rule widely increase the reach of European Union Law since it not only applies to the processing of data in the context of the activities of establishments of a controller or a processor in the Union, regardless of the nature of the processing, but also to a controller or processor not established in the Union if they offer goods or services to data subjects in the Union or if they perform activities that affect them like, for instance, if they profile a natural person, "*particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes*" (Recital 24).

This amplifies the range of European Union Law provisions on data protection to anyone who is doing business or envisages doing business in the European Union, turning the GDPR into a potential "global legal regime" in line with the European Union role as a "global actor". Therefore, establishments should be aware and respect GDPR whenever they process data that branches over to the European Union.

The primary relevant connecting factor is in line with the case law of the European Court of Justice since it applies to processing in connection with the activities of an establishment in the EU regardless of where the processing happens (*e.g.,* cloud storage abroad) [14]. Indeed, a flexible definition of "establishment" and a broad approach on territoriality was already given by the Court of Justice in the Google Spain and Google and Weltimo cases, although under the Directive framework [15].

The second clause for extraterritorial jurisdiction, in which the controller or processor are not established in the Union, are not, in our view, merely effects based since they entail a link, though tenuous as it may be in some cases, to the European Union, given that data subjects should be in the Union [16]. By extend-

---

by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law like, for instance, within consular posts or embassies. A. DE SOUSA GONÇALVES, *The extraterritorial application of the EU Directive on data protection* (2015) 19 *Spanish Yearbook of International Law*, 202, states that "*in these situations, data protection legislation does not have a truly extraterritorial application, since the application of the law of a Member State in a third State results from public international law and occurs in circumscribed cases*".

[14] Cf. S. BU-PASHA, *Cross-border issues under EU data protection law with regards to personal data protection* (2017) 16 (3) *Information & Communications Technology Law*, 218. According to A. AZZI, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation* (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 128, no more mental gymnastics is required since the EU rules apply "*regardless of whether the processing takes place in the EU*.".

[15] Respectively, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECJ, 13.5.2014 and Case C-230/14, Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, ECJ, 1.10.2015.

[16] It involves, therefore, a clear protective aim that is increasingly accepted in the fundamental

ing jurisdiction, it aims to avoid the interpretative problems raised by Article 4 of the Directive when confronted with cases in which intermediaries seek to avoid jurisdiction of courts by referring to the corporate structure and "means" adopted [17].

But this clause also incorporates the own line of thought and genuine policy of the European Union regarding the extension of its legislative and adjudicative powers [18].

On this note, one should be aware that extraterritoriality is no longer an exception in the international arena [19], and though it is not, nor should it be, the rule, it is a recurring feature in many situations that involve fundamental rights, environmental concerns and/or relevant political aims [20].

---

rights field for all persons, not only European Union Citizens or residents in the European Union (cf., on the widening of jurisdiction on the basis of fundamental rights protection, M. DEN HEIJER - R. LAWSON, *Extraterritorial Human Rights and the Concept of "Jurisdiction", Global Justice, State Duties – The Extraterritorial Scope of Economic,* M. LANGFORD-W. VANDENHOLE-M. SCHEININ-W. VAN GENUGTEN (eds.), *Social and Cultural Rights in International Law* (New York 2013), 153-191). In another approach this is seen as a more "market-place" oriented principle (cf. D. MOURA VICENTE-S. DE VASCONCELOS CASIMIRO, *Data Protection in the Internet: General Report* (Berlin 2020), 33).

Stating that this is an effects based clause because it puts focus on the potential harmful conduct and discards the location of the processing, cf. A. AZZI, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation* (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 131. B. VAN ALSENOY, *Reconciling the (extra)territorial reach of the GDPR with public international law*, G. VERMEULEN-E. LIEVENS (eds.), *Data Protection and Privacy under Pressure – Transatlantic tensions, EU Surveilance and Big Data* (Antwerp 2017), 97, considers that this provision entails a combination of the objective territoriality and the effects doctrine.

[17] C. KUNER, *Data Protection Law and International Jurisdiction on the Internet (Part 2)* (2010) 18 (3) *International Journal of Law and Information Technology*, 240, defended that "*the European Commission should consider revising Article 4(1) (c) to focus it away from the use of in the EU, and more towards the targeting criteria of Article 15(1) of the Brussels I Regulation, although it can be difficult to determine when an online activity is 'targeted' or 'addressed' at a particular State*". Cf, under the same line, L. MOEREL, *The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?* (2011) 1 (1) *International Data Privacy Law*, 28-46. GDPR, according to whom the relevance of the location of the equipment is replaced by a focus on people in the EU.

[18] E. USTARAN, *The Scope of Application of EU Data Protection Law and Its Extraterritorial Reach*, N. ISMAIL-E.L. YONG CIEH (eds.), *Beyond Data Protection – Strategic Case Studies and Practical Guidance* (Berlin 2013), 135- 156, dwells on the evolution of data protection regulation in the European Union in order to reach a right balance and the policy objectives of the European Union legislators.

[19] As defended, for instance, by L. STRISOWER, *L'Exterritorialité et ses Principales Applications,* ACADÉMIE DE DROIT INTERNATIONAL DE LA HAYE (eds.), *Recueil des Cours* (Paris 1925) I, 233.

[20] STEFANO BATTINI considers that the international interdependence converts extraterritoriali-

Jurisdiction is no longer, if it ever was, understood as an incidence of power over a certain territory. It is necessary to complement this dimension with the personal and functional aims of jurisdiction, which allows for jurisdiction based on the principles of nationality (active and passive), protection, universality and nowadays effects [21].

However, there must be a *genuine link* that respects the standards of international law for a state to legitimately assume jurisdiction [22] or a *reasonableness test* according to which the same conclusions are reached [23]. Criteria that seem to have been respected by Article 3 of the GDPR since the aim of this regulation is to ensure an effective protection of data subjects within the European Union, fulfilling its commitment as a fundamental rights organisation [24].

It is naturally expected that the more extraterritorial jurisdiction is accept-

---

ty into a non excepcional phenomenon, and that extraterritoriality *de iure* aims to contradict the impacts of an inevatible extraterritoriality *de facto*, (S. BATTINI, *Extraterritoriality: an Unexceptional Exception* (2008) *Séminaire de droit administratif, européen et global "Extraterritoriality and Administrative Law", 9* available at http://www.sciencespo.fr/chaire-madp/sites/sciencespo.fr.chaire-madp/files/stefano_battini.pdf, and S. BATTINI, *Globalisation and Extraterritoriality: an Unexceptional Exception,* G. ANTHONY-J. B. AUBY-J. MORISON-T. ZWART (eds.), *Values in Global Administrative Law* (Oxford 2011), 67).

On the role of *internet* in reconfiguring extraterritorial jurisdiction, cfr. T. SCHULTZ, *Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface* (2008) 19 (4) *The European Journal of International Law,* 799-839; and D. JERKER-B. SVANTESSON, *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation* (2015) 5 (4) *International Data Privacy Law*, 227.

[21] In general, on these principles cf., M. AKEHURST, *Jurisdiction in International Law* (1972 - 1973) 46 *British Yearbook of International Law*, 152-166, and C. RYNGAERT, *Jurisdiction in International Law* (Oxford 2015) 2nd ed., 104-141.

On the data protection field, cf. C. KUNER, *Data Protection Law and International Jurisdiction on the Internet (Part I*) (2010) 18 (2) *International Journal of Law and Information Technology*, 176-193, and ID, *Data Protection Law and International Jurisdiction on the Internet (Part II)* (2010) 18 (3) *International Journal of Law and Information Technology,* 227-247.

[22] F.A. MANN, *The Doctrine of Jurisdiction in International Law* (1973) *Studies in International Law,* 37.

[23] C. RYNGAERT, *Jurisdiction – Towards a Reasonableness Test*, M. LANGFORD-W. VANDENHOLE-M. SCHEININ-W. VAN GENUGTEN (eds.), *Global Justice, State Duties – The Extraterritorial Acope of Economic, Social and Cultural Rights in International Law* (New York 2013), 192-211.

[24] We agree in this part with P. DE HERT-M. CZERNIAWSKI, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context* (2016) 6 (3) *International Data Privacy Law*, 231. Against, C. KUNER, *The European Union and the Search for an International Data Protection Framework* (2014) 2 (1) *Groningen Journal ofInternational Law*, 55-71, and D. SVANTESSON, *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation* (2015) 5 (4) *International Data Privacy Law,* 234, that allude to the imposition of a privacy model on other jurisdictions instead of contributing to creation of better global privacy standards.

ed, the more political and legal conflict will increase [25], taken that the same conduct might trigger several jurisdiction clauses. This concurrence of jurisdiction is common in the international arena [26], and though international law does not provide a resolution framework for these cases, it has led to a certain international convergence movement in protecting fundamental data protection rights by public and private entities, all of which is welcomed and to which GDPR has widely contributed.

Comparing Article 3 GDPR provision with the former Article 4 of the preceding Directive, it seems clear that the GDPR no longer contains a conflict-of-laws provision determining the applicable law of a particular Member State for the processing of personal data [27]. It now includes a unified set of rules that Member States directly apply without need for further implementation to their national legislations, except certain situations. The scope of application of GDPR provisions is therefore defined in a self-limited way. This means that GDPR provisions will be applicable to all situations that involve data processing that fall under Article 3 unilateral conditions. Taking an international contract on services provision that states that personal data processing is regulated according to a non-European Member-State legislation, and where such data processing impacts data subjects located in the European Union, GDPR norms should nonetheless be applicable.

This points out to the qualification of the relevant provisions as overriding mandatory provisions, taking into consideration the definition in Article 9 of the Rome I Regulation. Indeed, they aim to safeguard fundamental political, economic and social interests on data protection common to Member States and to the European Union, which provides them with an imperative weight in international situations. And if this characterisation was already envisaged regarding Article 4 of Directive [28], it is now clear from both the wording and the

---

[25] I. JALLES, *Extraterritorialidade e Comércio Internacional – Um Exercício de Direito Americano* (Lisboa 1988), 205-208.

[26] F.A. MANN, *The Doctrine of Jurisdiction in International Law* (1973) *Studies in International Law,* 3.

[27] M. BRKAN, *Data Protection and Conflict-of-laws: A Challenging Relationship* (2016) 13 *European Data Protection Law Review,* 336, points that out since the regulation itself unifies the legal regime on processing of data.

[28] C. PILTZ, *Rechtswahlfreiheit im Datenschutzrecht?* (2012) *K&R – Kommunikation & Recht*, 640-645; M. BRKAN, *Data Protection and Conflict-of-laws: A Challenging Relationship* (2016) 13 *European Data Protection Law Review,* 333-334. Arguing that this characterisation had not been cleared by the European Court of Justice, cf. I. REVOLIDIS, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?* (2017) 11 (1) *Masaryk University Journal of Law and Technology,* 12. We believe, however, that judgment Case C-191/15, Verein für Konsumenteninformation v Amazon EU Sàrl, ECJ, 28.7.2016 sufficiently supports this characterisation.

teleology of Article 3 GDPR that it is the rightful one [29].

However, as Jiahong Chen clearly states, this is not the end of the story since there are still remaining problems of applicable national law once the GDPR continues to leave relevant areas for national interpretation and further regulation (or derogations) from Member States, which, for that Author, creates a serious loophole that could possibly cancel out most of the improvements brought by the reform [30].

Although we agree that it might have been clearer to establish conflict of law rules in cases where diversity between Member States is allowed for, we do not believe that the situation is as calamitous as it is made out to be.

The application of the GDPR itself may not respond sufficiently or clearly to all questions relevant to Court proceedings or to related questions. However, in a situation in which there is a contract between the data subject and the data controller, it is acknowledged that the Rome I Regulation will provide sufficient guidance on the choice of applicable law. However, the application of Rome II Regulation to these cases in non-contractual situations continues to be a grey zone given the fact that it is not applicable to privacy issues [31].

---

[29] P.A. DE MIGUEL ASENSIO, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation* (2017) 69 (1) *Revista Española de Derecho Internacional,* 104.

[30] J. CHEN, *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation* (2016) 6 (4) *International Data Privacy Law,* 311-316.

[31] Article 1(2) of the Rome II Regulation provides that '*[t]he following shall be excluded from the scope of this Regulation: [. . .] (g) non-contractual obligations arising out of violations of privacy and rights relating to per- sonality, including defamation'.* J. CHEN, *How the best-laid plans go awry: the (unsolved) issues of applicable law in the General Data Protection Regulation* (2016) 6 (4) *International Data Privacy Law,* 319, argues that even if the Charter distinguishes between these two rights (right to data protection and right to privacy), it is very difficult to separate them in Courts, because we "*will need a handle on the traditional tort law system in order to translate the language of data protection law into the language of private law. Without such a handle – right to privacy – the claim of breach of data protection can hardly find its way into the private law system*". P. HUSTINX, *EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation*, M. CREMONA (eds.), *New Technologies and the Law* (Oxford 2017), 172, takes a different view and proposes that article 8 of the Charter to reach its fullest potential should be better distinguished from article 7, meaning that "*Article 8, involving all processing of personal data, should not be confused with the question of wether the fundamental right to data protection has been interfered with*". Along the same line, cf. J. KOKOTT-C. SOBOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR* (2013) 3 (4) *International Data Privacy Law*, 222-228; O. LYNSKEY, *Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order* (2014) 63 (3) *International and Comparative Law Quarterly*, 569-597; and G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Berlin 2014), 268-272.

Going against the mainstream current [32], we believe that the Rome II Regulation should govern non-contractual issues related to data protection. Indeed, long before this Regulation was passed, Directive 95/46/EC already established a conflict-of-laws provision that explicitly governed data privacy [see, among many others, recital 11 and article 1(1)] [33]. This Directive is even mentioned in the Rome II Regulation (Article 30, review clause), but was not directly affected by it (Article 27) [34]. The conclusion possible is, henceforth, that the concept of privacy incorporated – after strong debate – in Article 1 (2) (d) of the Rome II Regulation did not include data privacy, by then governed by Directive 95/46/EC and the implementing laws of the Member States. This conclusion goes along the lines of the debate in which the main issues at stake in the Rome II Regulation were more "traditional" violations to privacy such as, for example, publications, defamation and slander in newspapers, magazines and, of course, the internet - all of which more related to freedom of the press and freedom of expression in other media than with data protection [35].

This means that when Directive 95/46/EC was repealed by the GDPR, the concept of privacy under the Rome II Regulation did not "expand" its scope to include data protection. In fact, as an exception to the general scope of application of this instrument, the concept of privacy should continue to be read as it once was, and not include matters that were (re)regulated by the European Union in the GDPR. Consequently, in the absence of a European Union Instrument that defines specific rules-of-conflict for data protection, the Rome II Regulation should apply to all non-contractual issues that were not fully harmonised by

---

[32] See for instance, U. GRUŠIC' ET AL., *Cheshire, North & Fawcett: Private International Law* (Oxford 2017) 15th ed., 798-799, according to which "The exclusion does however extend to violations of data protection laws"; and D. MOURA VICENTE-S. DE VASCONCELOS CASIMIRO, *Data Protection in the Internet: General Report* (Berlin 2020), 37-38. Less stringently, see A. DICKINSON, *The Rome II Regulation – The Law Applicable to Non-Contractual Obligations* (Oxford 2008), 240 and P. A. DE MIGUEL ASENSIO, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation* (2017) 69 (1) *Revista Española de Derecho Internacional,* 105.

[33] A concept that has been developed and that does equate fully with the right to privacy. Cf. the seminal study of L. A. BYGRAVE, *Data Privacy Law: An International Perspective* (Oxford 2013). To mark the distinction between privacy and data protection, in the GDPR reference to privacy has been omitted entirely. Which, from our point of view, is an indicator of an increasing distinction, both doctrinal and legislative, of both concepts.

[34] Indeed, the proposal of the European Parliament in the 1st and 2nd reading positions that extended the special rule to "violations of privacy or of rights relating to the personality resulting from the handling of data protection" did not survive the legislative process.

[35] See, among many others, J. MEEUSEN, *Rome II: A True Piece of Community Law,* J. AHERN-W. BINCHY (eds.), *The Rome II Regulation on the Law Applicable to Non-Contractual Obligations – A New International Litigation Regime* (Boston 2009), 15.

the GDPR and that were not excluded from the scope of application of Rom-II Regulation.

This is, in our opinion, the only reading that salvages the teleological and autonomous interpretation of the concepts of European Union Law [36], to which the European Union and Member-States are bound and the one that puts an end to countless controversies and divergences in the field [37]. And if the application of the Rome II Regulation to some aspects of data protection may cause fragmentation of the applicable law, given the fact that the *loci damni* can be widespread [38], it will at least give clarity on many other issues that would have otherwise had to be solved under the also divergent applicable international private rules of the Member-States.

One of the main refractions of this scope of application resides in Article 82 (right to compensation and liability) that defines specific rules to allow for private enforcement of the GDPR. It clearly states that any person who has suffered material or non-material damage as a result of an infringement of GDPR rules have the right to receive compensation from the controller or processor for the damage suffered. This points out that GDPR and other European Union provisions will also be the guiding criteria in non-contractual matters.

4. International data transfers

In what regards transfer of data from the European Union to third countries and international organisations, it is established that both Union and Member States might conclude international agreements as long as such agreements respect GDPR and other European Union provisions on data protection. They should, therefore, guarantee an appropriate level of protection for the fundamental rights of the data subjects (Recital 102).

---

[36] Indeed, the wording of the provision of Rome II, which only refers to privacy, its history and background (media violations and non-technical aspects of data protection), the systematic context in which the provision is found, including its relation to other provisions in other European Union instruments (at the time the Directive that explicitly regulated data privacy), and the objectives of the provision in question and the objectives and scheme of the overall Regulation, that aims to be a general scheme on all non-contractual obligations, point out the fact that it now includes data protection issues.

[37] Therefore, unlike what is defended by H. HIJMANS, *The European Union as Guardian of Internet Privacy the Story of Art 16 TFEU* (Berlin 2016), 66-68, there are relevant legal effects in distinguishing between privacy and data protection on the internet.

[38] For an analysis on this issue, cf. D. SVANTESSON, *Rome II Regulation and Choice of Law in Internet-Bases Violations of Privacy and Personality Rights - On the Wrong Track, but in the Right Direction* (2011) 16 *Austrian Review of International and European Law,* 275-298.

The relevance of this level of protection goes so far as to impeding the recognition of enforcement of decisions of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data when it is not frameworked by an international agreement such as a mutual assistance treaty, or other grounds of transfer included in the GDPR (Article 48).

This means that international agreements are not the only basis for international transfer of personal data and allows for other mechanisms of unilateral or contractual nature to take place; instruments that, it should be emphasized, require no previous agreement between States. The other grounds for transfer mentioned in the Regulation include the issuance of adequacy decisions, appropriate safeguards and derogations for specific situations.

Adequacy decisions are implementing decisions from the Commission with binding effect for the entire Union that establish that a third country, a territory or specified sector within a third country, or an international organisation offer an adequate level of data protection (Article 45). The adoption of such decisions involves a lengthy and complex process and is mainly why, at the time of this writing only these third countries ensured an adequate level of protection: Andorra, Argentina, Canada (commercial organisations) Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay (private sector organisations) and the USA (if the recipient belongs to the Privacy Shield) [39].

The agreements and adequacy decisions on data protection have been subject to criticism, mostly in what involves data protection transfers between the European Union and the United States. In the wake of the Schrems "saga", the Court of Justice decided that Commission's Decision 2000/520/EC of 26 July 2000, regarding the adequacy of the protection provided by the safe harbour privacy principles, was invalid since the appropriate level of protection required by European Union data protection law (at the time the Directive) was not met. Furthermore, the protection granted was not general and interference from United States authorities was permitted given the prevalence of the United States public interest; additionally, restrictions were not proportional with no adequacy and necessity in the identification of storable data [40].

---

[39] Cf. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[40] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECJ, 6.10.2015. This case is also of great relevance to the competencies of the Supervisory Authorities since while they are bound by the Commission's Decision when considered valid, this shouldn't prevent them from fully using their investigative powers when facing claims on the (in)adequacy of protection afforded by third countries.

In general, these difficulties to meet the requirements of data protection in the European Union opened the door to alternative forms of demonstrating that respect in a "case by case" basis. The finding that a third country itself ensures a level of protection essentially equivalent to that imposed by European Union law and that, as a consequence, personal data may be transferred to that country without the controller being required to obtain specific authorisation, has proven to be quite difficult [41].

In this case, appropriate safeguards should apply in the absence of an international agreement and an adequacy decision to allow for a controller or processor to transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available (Article 46). This implies that a set of instruments that include binding corporate rules, standard data protection clauses, approved codes of conduct or approved certification mechanism that ensure an appropriate level of data protection are available for public and private data importers.

These tools basically rely on a contractual commitment undertaken by a third state data importer to conform to a set of obligations relating to the processing of data that comply with the GDPR provisions and whose respect must be safeguarded both by the data-importer and the data-exporter. Also, since these contracts must confer effective legal remedies, the data subject is usually considered a beneficiary of the contract in order to be able to react against both the data importer and/or exporter. These contracts, though usually private in nature, require a public element given that they have to be approved by a national supervisory authority who is called to assess the existence of appropriate safeguards and means of redress [42].

But again, despite its practical relevance [43], this mechanism has not been

[41] C. KUNER, *Developing an Adequate Legal Framework for International Data Transfers*, S. GUTWIRTH ET AL. (eds.), *Reinventing Data Protection?* (Berlin 2009), 263-273 proposed that, given the difficulties in reaching adequacy decisions (length and complexity, political tensions, overload and lack of means for the adequacy assessment), there should be other ways to prevent circumvention of European Union law under an accountability standard.

[42] We agree with M. MANTOVANI, *Contractual Obligations as a Tool for International Transfers of Personal Data* (2020) availabe at https://eapil.org/2020/01/20/contractual-obligations-as-a-tool-for-international-transfers-of-personal-data/, that this does not change the civil and commercial nature of most contracts as they are usually linked to other contractual arrangements between the parties. Also, like the author we believe that this is a relevant governance tool since it allows for a wider acceptance *from within* of European Union data protection standards and contribute to its dissemination in areas outside of its normal reach.

[43] The most popular method by far for data transfers outside the EU is the use of standard contractual clauses (88% of respondents), followed by compliance with the EU-U.S. Privacy Shield arrangement (60%), according to the IAPP-EY Annual Governance Report 2019, available at https://iapp.org/store/books/a191P000003Qv5xQAC/.

well received. At the time of completing this paper, a decision is pending in the Court of Justice (the so called Schrems II case) against the Commission Implementing Decision (EU) 2016/1250 – EU-U.S. Privacy Shield –, that is applicable to data transfers between the European Union and the United States. However, it is also aimed against the Commission Decision 2010/87/EU, of 5 February 2010, regarding standard contractual clauses for the transfer of personal data to processors established in third countries.

In this case, Advocate General SAUGMANDSGAARD ØE, taking into consideration the GDPR provisions, considered, in 19 December 2019, that the standard contractual clauses framework is sufficient. In situations where the safeguards in the standard contractual clauses may be reduced or eliminated (for instance when the law of the third country of destination imposes obligations that are contrary to the requirements of those clauses on the importer or edits blocking Statutes), it should be, on a case-by-case basis, up to the controller or, when it discharges its obligations, up to the supervisory authority to examine the situation and, if necessary, to prohibit or suspend such transfers. Additionally, if the Supervisory Authority does not exercise its corrective competences under the GDPR, it may be subject to a judicial action from the complainants, given its reduced discretionary powers on this field [44].

Furthermore, GDPR also allows for derogations for specific situations in a very similar fashion to what was already established in the Directive. In this case a transfer or a set of transfers of personal data to a third country or an international organisation will take place only on the basis of typified justifications laid down in Article 49 GDPR. The most important of these derogations in quantitative terms is the explicit consent of the data subject to the proposed transfer, but other relevant clauses, with underlying private or public concerns, are also established. Given that these are derogations, they must be last resort and occasional according to their exceptional nature as established in Guidelines 2/2018 on derogations of Article 49 [45].

---

[44] Case C-311/18, Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems, ECJ, 9.5.2018. In what regards the Privacy Shield Adequacy Decision, the Advocate General has argued for the practical irrelevance of its invalidity analysis. However, this raises doubts in what regards the safeguards around the equivalence of the United States surveillance measures and the role of the Privacy Ombudsperson: if they can indeed compensate for insufficiencies of the judicial protection afforded to individuals whose data is transferred to the United States. For other criticism on this framework, see S. BU-PASHA, *Cross-border issues under EU data protection law with regards to personal data protection* (2017) 26 (3) *Information & Communications Technology Law,* 224 - 227. There is also another case pending before the General Court Case T-738/16, La Quadrature du Net and Others v Commission, GC, 25.10.2016 only directed towards the Privacy Shield Framework.

[45] GDPR additionally offers a last resort mechanism [Article 49 (1) last paragraph] according to which, when none of the above-mentioned exist "*a transfer to a third country or an interna-*

There are, therefore, several ways to framework international transfer of data that go far beyond the typical public international law mechanisms and that allow for unilateral decisions and contractual arrangements in the field. These should, however, be justified and comply with the appropriate level of data protection set forth in the GDPR, which will be under the control of the Supervisory Authorities, the focus of our analysis at present.

5. The supervisory mechanism

With more responsibility comes more supervision. Therefore, the role of supervisory authorities and the personal data supervisory mechanism is essential to the design of the GDPR.

The Court of Justice has previously ascertained that the supervisory authorities are the guardians of fundamental rights and freedoms put at stake by data processing operations and, therefore, their independence is an essential element of their protection and cannot be restricted in any way [Article 8 (3) of the Charter] [46].

Supervisory authority or Data Protection Authority (DPA) is a "mandatory" independent public authority established in each State which is concerned by the monitoring of the processing of personal data because "*(a) the controller or processor is established in the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority*" [Article 4 (22)].

The tasks of each supervisory authority are defined in Article 57. The number and nature of such tasks are impressive. They range from: monitoring and enforcement, providing information to private and public entities, raising cooperation awareness, handling and investigating complaints, adopting standard contractual clauses, encouraging the drawing up of codes of conduct, approving binding corporate rules, authorising contractual clauses and provisions, and act-

tional organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data".

[46] On this issue, Case C-518/07, European Commission v Federal Republic of Germany, ECJ, 9.3.2010; Case C-614/10, European Commission v Republic of Austria, ECJ, 16.10.2012; Case C-288/12, European Commission v Austria, ECJ, 8.4.2014.

ing in certification and accreditation procedures. Correspondingly, the powers of such authorities are very wide and allow for various forms of investigation and audits: the imposition of fines or other penalties or of temporary or definitive limitation including a ban on processing or suspension of international data flows, the ordering of rectification or erasing of personal data and the withdrawal of certifications, etc.

This is a relevant difference regarding the Directive since it has already imposed on states a minimum status for their supervisory authorities (Article 28), but the powers entailed were not as broad nor as intrusive as the ones established in the GDPR [47]. A definitive option towards strong and legally well-equipped supervisory authorities was made because the implementation of all mechanisms established in the GDPR so require.

Furthermore, considering that a great number of situations involve data protection issues and concerns in many member states, GDPR defines which authority should be the lead in each case to enable a more effective monitoring and control of GDPR rules as well as to detect and pursue eventual infractions. This "one-stop-shop" system aims to enable more than just mere cooperation obligations between supervisory authorities [like the ones previewed in Article 28 (6) of Directive] [48], since it represents an institutionalisation of common and integrated procedures between member states that might lead to the adoption of decisions with transnational effects, that should be automatically recognised in other member states [49].

---

[47] According to the Final Report of the European Commission on the Comparative Study of Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments, of 20 January 2010, pp. 43-44, available at https://op.europa.eu/en/publication-detail/-/publication/9c7a02b9-ecba-405e-8d93-a1a8989f128b, "*DPAs have great insight and knowledge, and provide helpful guidance on the law - but they are not effective in terms of enforcement: "Policing" of data protection compliance by DPAs is generally weak and ineffective*".

[48] The GDPR's cooperation and consistency mechanism only applies to controllers with an establishment, or establishments, within the European Union. If the company does not have an establishment in the EU, the mere presence of a representative in a member state does not trigger the one-stop-shop system. This means that controllers without any establishment in the EU must deal with local supervisory authorities in every member state they are active in, through their local representative. However, there are relevant doubts as to whether those representatives can be subject to enforcement proceedings in the event of non-compliance by the controller or processor. This is mentioned in Recital 80 but not provided for in the binding articles of the Regulation, so there is controversy as to whether a representative may incur some sort of liability, in addition to the operator (on this, cf. A. AZZI, *The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation* (2018) 9 *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 133).

[49] This might be particularly relevant on de-referencing decisions, in which a mere territorial effect might not suffice to guarantee the effective and complete protection of data subjects' rights since it shouldn't necessarily be restricted to national domains. In this situation, the European

Article 56 establishes as lead supervisory authority the one of the main establishment or of the single establishment of the controller or processor [50], except when processing is carried out by public authorities or private bodies acting in the public interest. In this case the supervisory authority of the member state concerned will always be competent, Article 55 (2).

As a lead supervisory authority, it takes up the instruction of the administrative procedure and conducts itself in such a way as to reach the highest level of consensus between the other Supervisory authorities concerned. Of course, the instruction phase of the procedure can be developed in articulation between these entities by the provision of mutual assistance (Article 61) and the conducting of joint operations (Article 62). But it is up to the lead supervisory authority to, after the necessary diligences and if the decision isn't urgent, case then Article 66 applies, to "*submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views*" – Article 60(2).

If this draft proposal is accepted or not opposed by the other concerned supervisory authorities, "*the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it*" (No. 6). In this case the "*The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision*" (No. 7). Therefore, the decision of the lead supervisory authority produces real transnational effects in other member states [51].

Court of Justice already ruled that a de-referencing in all search engines might not be necessary and proportional; however, it pointed out the necessity of balancing of competing rights by the controller and of cooperation between supervisory authorities in order to reach a consensus and a single decision which is binding on all those authorities and the controller [Case C- 507/17, Google LLC, ECJ, 24.9.2019, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)]. For a comment on this case, cf. Y. MIADZVETSKAYA- G. VAN CALSTER, *Google at the Kirchberg Dock. On Delisting Requests, and on the Territorial Reach of the EU's GDPR* (2020) 1 *European Data Protection Law Review,* 143-151.

[50] If there are doubts regarding this issue, it is up to the Board to adopt a binding decision on which of the supervisory authorities concerned is competent for the main establishment [Article 65 (1) (b)]. In order to avoid some of these doubts, the Article 29 Data Protection Working Party has issued guidelines for identifying a controller or processor's lead supervisory authority on 13 December 2016, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235.

[51] On transnational acts and their effects, see J. RODRIGUEZ-A. MUÑOZ (eds.), *Recognition of Foreign Administrative Acts* (Berlin 2015) and D. LOPES, *Eficácia, Reconhecimento e Execução de Actos Administrativos Estrangeiros* (Coimbra 2018), 339 ff.

In cases where one or more of the other concerned supervisory authorities expresses a relevant and reasoned objection to the draft decision, two possibilities open. If the lead supervisory authority does not agree with such objection, a consistency mechanism is in order [article 60 (4)] and a dispute resolution by the Board takes place (article 65). Within this procedure, the European Data Protection Board adopts a binding decision on the matter that is reported to the supervisory authorities and to the Commission. However, it is up to the lead supervisory authority or, as the case may be, the supervisory authority with which the complaint has been lodged to adopt its final decision on the basis of the Board's decision that should be attached to it.

In the case where the lead supervisory authority intends to follow the relevant and reasoned objection made, it submits a revised draft decision for their opinion [Article 60 (5)] to the other supervisory authorities concerned. Nevertheless, if a concerned Supervisory Authority still objects, the consistency mechanism also applies.

These new forms of mixed administration raise questions of justiciability of the decisions taken since the right to an effective judicial remedy should be, in principle, directed towards the decisions of the Supervisory authorities (Article 78) even in cases in which they are preceded by an opinion or a decision of the Board in the consistency mechanism [knowing that the Board is a body of the Union and has legal personality, Article 68(1) GDPR]. Though in these cases the opinion or decision of the Board should be forwarded to the Court and, therefore, should be taken into consideration, the appraisal of their validity will be out of the national Courts reach since they are pledged, in these cases, to ask for a preliminary ruling from the Court of Justice.

There are areas, however, that are still dependent upon "nationalised" indirect administration: administrative fines and other penalties. Nevertheless, in order to reinforce supervisory authorities powers, general conditions for imposing administrative fines are established in the GDPR (article 83) [52] and other penalties, usually of criminal nature, are explicitly allowed for (article 84) [53].

Another aspect that merits attention is the fact that these supervisory rules do not extend as far as the material scope of GDPR, and leave international enforcement [54] mainly to international cooperation efforts [55] and prin-

[52] Article 29 Data Protection Working Party has issued guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, 3 October 2017, available at https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

[53] However, there is no harmonisation of the use of criminal sanctions. Cf. P. DE HERT, *The EU data protection reform and the (forgotten) use of criminal sanctions* (2014) 4 *International Data Privacy Law,* 262-268.

[54] Though extraterritorial prescriptive jurisdiction has augmented, this tendency has been less

cipally to the adjustment of controllers and processors to a high level of data protection.

6. International civil and administrative procedural law

Regarding international civil and administrative procedural law, GDPR establishes special rules on jurisdiction that show how far the European Union has come in trying to complement private and public enforcement in data protection issues [56].

In the first case, the right to an effective judicial remedy against a controller or processor should be brought before the courts of the member state where the controller or processor has an establishment. Alternatively, such proceedings based on the material scope of the GDPR may be brought before the courts of the member state where the data subject has his or her habitual residence unless the controller or processor is a public authority of a member state acting in the exercise of its public powers (Article 79).

There is, therefore, alternativeness between these two grounds for jurisdiction. The data subject should choose, if those grounds are not coincidental, which is more favourable: if the courts of the place of establishment where an enforcement of the decision might be easier to practically accomplish [57], if the courts of his/her habitual residence taking into consideration, for instance, the knowledge of the judicial system and the language factor.

---

visible and effective in what regards enforcement jurisdiction. Therefore, it is common in the international arena that there is prescription without enforcement. Cf. D. W. BOWETT, *Jurisdiction: Changing Patterns of Authority over Activities and Resources* (1982) 53 *The British Yearbook of International Law,* 1 and P. VAN SLOT-E. GRABANDT, *Extraterritoriality and Jurisdiction* (1986) 23 (3) *Common Market Law Review,* 548.

[55] There are, nonetheless, cases in which states cooperate in the enforcement of foreign administrative decisions as in the internet arena, for example. Cf. B. H. OXMAN, *Jurisdiction of States*, R. WOLFRUM (eds.), *The Max Planck Encyclopedia of Public International Law* (Oxford 2012) 6, 547 and H.L. BUXBAUM, *Territory, Territoriality, and the Resolution of Jurisdictional Conflict* (2009) 57 *The American Journal of Comparative Law,* 673.

[56] Nevertheless, the judicial and administrative lines of jurisdiction are not sufficiently interconnected, which means that a full protection of data subject rights may depend on initiating both (cf. P.A. DE MIGUEL ASENSIO, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation* (2017) 69 (1) *Revista Española de Derecho Internacional,* 92).

[57] It should be noted that a Member State judgment concerning "civil and commercial matters", can nonetheless, be recognized and enforced in the other European Union Member States as well as Norway, Iceland and Switzerland, under Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters or the 2007 Lugano Convention.

Questions still arise regarding the relation between this specific provision and the European Union Regulations. The wording of recital 147 – "*(w)here specific rules on jurisdiction are contained in this Regulation, in particular as regards proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council (13) should not prejudice the application of such specific rules*" is not clear on this behalf[58].

It is arguable if, besides the GDPR, also general rules on jurisdiction may apply, being the "*actor sequitur forum rei*" principle the most relevant. Since the objective of the GDPR is to provide a wide range of guarantees for data subjects, we tend to agree with Lundstedt that these grounds do not supplant but supplement the general rules on jurisdiction[59]. One thing is certain, general rules that contradict the jurisdictional grounds laid down in Article 79 are not admissible as, for instance agreements that establish exclusive choice of court clauses[60].

Regarding administrative procedures, Article 78 enshrines the right to an ef-

---

[58] Also, article 67 of Regulation (EU) No 1215/2012 stipulates that it "*shall not prejudice the application of provisions governing jurisdiction and the recognition and enforcement of judgments in specific matters which are contained in instruments of the Union*".

[59] L. LUNDSTEDT, *International Jurisdiction over Cross-border Private Enforcement Actions under the GDPR* (2018) 57 *Stockholm Faculty of Law Research Paper Series*, 253*,* available at *https://ssrn.com/abstract=3159854;* also P.A. DE MIGUEL ASENSIO, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation* (2017) 69 (1) *Revista Española de Derecho Internacional,* 99-100. IOANNIS REVOLIDIS, *Judicial Jurisdiction Over Internet Privacy Violations and the GDPR: A Case of "Privacy Tourism"?* (2017) 11 (1) *Masaryk University Journal of Law and Technology,* 22-23, remarks that, applied together, GDPR and Brussels Ia [Article 7(2)] would create a multitude of different *fora* in favour of the data subject, which would be detrimental to the administration of justice within the European Union, at least until clarification from the Court of Justice. This profusion of possible competent *fora* was not ignored by the GDPR, which set rules on suspension of proceedings, whenever more than one court of a member state was seized concerning the same subject matter (article 81). According to M. REQUEJO ISIDRO, *Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection* (2019) 3 *Max Planck Institute Luxembourg for Procedural Law Research Paper Series* available at https://ssrn.com/abstract=3339180, the wording of this provision is "*all inclusive: at least at first sight it could be equally applied to judicial proceedings for a remedy against a decision of a supervisory authority, or for a civil remedy between private parties*". Against, P.A. DE MIGUEL ASENSIO, *Jurisdiction and Applicable Law in the New EU General Data Protection Regulation* (2017) 69 (1) *Revista Española de Derecho Internacional,* 102-103, sees it as a rule only applicable in procedures against supervisory authorities since in civil claims Articles 29 and 30 of Regulation (EU) No 1215/2012 should be deemed applicable.

[60] However, jurisdictional clauses as such are not forbidden, if they are not exclusive. They might also help to identify connecting factors and in particular those regarding the location of the establishments of the controller or processor contributing, therefore, to legal certainty (cf. F. FANGFEI WANG, *Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction* (2013) 24 *European Business Law Review*, 616).

fective judicial remedy against a legally binding decision of a supervisory authority concerning them, plus the right to an effective judicial remedy where the supervisory authority does not handle a complaint or does not inform the data subject on the progress or outcome of the complaint lodged within three months [61].

Therefore, not only actions but also omissions should merit a specific judicial response from the member state where such supervisory authority is established. This is particularly relevant in cases of complaints as, for instance, regarding data transfers that are not appropriately investigated and eventually pursued by supervisory authorities. In sum, in the data protection area a full jurisdictional review in administrative matters should be available and entails the possibility of analysing in matters of fact and law decisions or omissions of the supervisory authorities [62].

Another important consequence of this provision is that, unlike what was allowed for under the Directive (and according to a decision of the Court of Justice) [63], national law should not require that the data subject first exhaust administrative remedies before bringing a court action against a Supervisory Authority. Of course other administrative or non-judicial remedies may exist; however they should do not prejudice the immediate right to an effective judicial remedy against such Authorities, which increases the "control" of data subjects regarding their data, escaping the eventual limitations (financial, administrative or others) of the competent Supervisory Authorities to handle their claims.

In any of these cases, where a data subject considers that his or her rights under this Regulation are infringed, he or she should have the right to mandate a not-for-profit body, organisation or association which is constituted in accordance with the law of a Member State, has statutory objectives which are in the

---

[61] This is a novelty of the GDPR imposing a fixed and uniformised deadline on handling complaints by member states and, therefore, innovating from the usual *lex fori* rule in administrative and procedural matters.

[62] This is seen as a form of furthering the accountability of these expert bodies and to contribute to good governance within the European Union (cf. H. HIJMANS, *The European Union as Guardian of Internet Privacy: the Story of Art 16 TFEU* (Berlin 2016), 376 and M. SZYDŁO, *Judicial review of decisions made by national regulatory authorities: Towards a more coherent application of EU sector-specific regulation* (2014) 12 (4) *International Constitutional Law Review*, 932).

Although no rule of recognition exists within the European Union regarding judicial decisions in administrative matters, it should me mentioned that the total or partial invalidity of a Supervisory Authority decision should have consequences in the other member states where it was recognised and eventually applied as a matter of consistency.

[63] Case C-73/16, Puškár, ECJ, 27.9.2017, in which the European Court of Justice did not in principle exclude the possibility for member states to establish mandatory administrative complaints before bringing a legal action, as long as they were not disproportionate and did not constitute an obstacle to the exercise of the right to a judicial remedy guaranteed by Article 47 of the Charter.

public interest and is active in the field of the protection of personal data[64], to lodge a complaint on his or her behalf with a supervisory authority, exercise the right to a judicial remedy on behalf of data subjects or even, if provided for in Member State law, exercise the right to receive compensation on behalf of data subjects (Article 80 and Recital 142).

This is also a leveling rule between Member States that tries to compensate for the usually atomistic and fragmentary nature of complaints (that, linked to the difficulties and costs of litigation, leads to a so far paucity of judicial claims) by allowing for collective actions, with all of the benefits this might bring, according to the law applicable, in terms of gathering of proof, court fees, and the simplification of procedures.

7. Conclusions

The preceding considerations lead us to what we believe to be self-evident: the ease in accessing personal data, mostly in an internet context, has changed traditional notions of applicable law and jurisdiction when in alliance with what are seen as admissible grounds for extending jurisdiction: fundamental rights. Also, it has changed perceptions on the distribution of regulatory authority between states and allowed for the introduction of new and flexible cooperation schemes between them and other public and private entities.

Although we agree that the traditional scheme of redress divided into three layers – data protection remedies sought before the data controller or processor; data protection remedies sought before supervisory authorities and data protection remedies sought before national courts – still needs improvement[65], we adopt the view that the solutions inserted into the GDPR constitute a sound basis for enhancing personal data protection. In fact, they bring tradition and modernity, distance and proximity, public and private closer together and adopt flexible forms of action both at an administrative and at a court level, which is highly desirable in the ubiquitous and pluriform data protection field.

---

[64] It should be noted, however, that Article 80 requirements lead to the conclusion that only entities that are regarded as private not for profit organisations will have the right to represent data subjects for these purposes, not other organisations such as consumer protection or professional related groups.

[65] Cf., among other critics, A. GALETTA-P. DE HERT, *The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System?* (2015) 8 (1) *Review of European Administrative Law*, 125-151 and M. REQUEJO ISIDRO, *Procedural Harmonization and Private Enforcement in the Area of Personal Data Protection* (2019) 3 *Max Planck Institute Luxembourg for Procedural Law Research Paper Series* available at https://ssrn.com/abstract=3339180.