AEDIPr, t. XVIII, 2018, pp. 163–192

Recibido: 3 octubre 2018
Aceptado: 1 diciembre 2018

LAW APPLICABLE TO PERSONAL DATA PROTECTION ON THE INTERNET: SOME PRIVATE INTERNATIONAL LAW ISSUES

Luís DE LIMA PINHEIRO *

ABSTRACT: Law Applicable to Personal Data Protection on the Internet: Some Private International Law Issues

In relationships with relevant contracts with more than one sovereign State (transnational relationships), personal data protection raises an issue of determination of the applicable law. The applicable law can either be a national law or a supranational instrument, which unifies or uniformizes the rules applicable in the States bound by it.

The Regulation (EU) no 2016/679, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR) laid down a developed body of uniform material rules on personal data protection. The problems of determination of the applicable law, however, are not suppressed. These problems are raised mainly at three levels: first, the determination of the spatial scope of application of the GDPR; second, the determination of the applicable law when the GDPR refers to the law of the Member States; and third, the determination of the national law applicable to issues that the GDPR does not govern, not even by reference, such as most of the issues relating to torts resulting from the breach of the GDPR provisions.

The aim of this essay is to provide a first approach to these problems and their solution on the internet context.

KEYWORDS: GENERAL DATA PROTECTION REGULATION – LAW APPLICABLE TO PERSONAL DATA PROTECTION –INTERNET – LAW APPLICABLE TO PERSONALITY RIGHTS – PERSONAL DATA PROTECTION – LAW APPLICABLE TO INTERNET TORTS.

RESUMEN: Ley aplicable a la protección de datos personales en internet: algunas cuestiones de derecho internacional privadas

En las relaciones con contratos relevantes con más de un Estado soberano (relaciones transnacionales), la protección de datos personales plantea un problema de determinación de la ley

* Full Professor at the Law School of the University of Lisbon.

ISSN 1578–3138
DOI: 10.19194/aedipr.18.05

aplicable. La ley aplicable puede ser una ley nacional o un instrumento supranacional, que unifica o uniformiza las normas aplicables en los Estados vinculados por ella.

El Reglamento (UE) no 2016/679, sobre la protección de personas físicas con respecto al procesamiento de datos personales y sobre la libre circulación de dichos datos (GDPR) estableció un cuerpo desarrollado de normas materiales uniformes sobre protección de datos personales. Los problemas de determinación de la ley aplicable, sin embargo, no se suprimen. Estos problemas se plantean principalmente en tres niveles: primero, la determinación del alcance espacial de la aplicación del GDPR; segundo, la determinación de la ley aplicable cuando el GDPR se refiere a la ley de los Estados miembros; y tercero, la determinación de la ley nacional aplicable a los asuntos que el GDPR no regula, ni siquiera por referencia, como la mayoría de los asuntos relacionados con los daños causados por el incumplimiento de las disposiciones del GDPR.

El objetivo de este ensayo es proporcionar un primer acercamiento a estos problemas y su solución en el contexto de Internet.

PALABRAS CLAVE: REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS – LEY APLICABLE A LA PROTECCIÓN DE DATOS PERSONALES – INTERNET – LEY APLICABLE A LOS DERECHOS DE LA PERSONALIDAD – PROTECCIÓN DE DATOS PERSONALES – LEY APLICABLE A LOS DAÑOS EN INTERNET.

I. Introduction

Personal data is information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[1].

Privacy is a value protected by democratic legal systems in general, but there are important differences concerning the content and reach of this protection, as well as, in particular, regarding its balance with the freedom of expression and information. These differences occur, namely, in the context of personal data protection[2].

In relationships with relevant contacts with more than one sovereign State (transnational relationships), personal data protection raises an issue of determination of the applicable law. The applicable law can either be a national law or a supranational instrument, which unifies or uniformizes the rules applicable in the States bound by it.

In the Portuguese legal order, *personal data protection is a fundamental right*, which not only derives from the right to privacy but also is, to a certain extent, autonomous.

[1] *Vid.* definition contained in Art. 4(1) of the General Data Protection Regulation.

[2] *Vid.* P. Schwartz and K.–N. Peifer, "Transatlantic Data Privacy", *LSN Cyberspace Law eJournal*, vol. 22, nº 85, 2017 (available in SSRN), pp. 121 ss.

The Portuguese Constitution enshrines the right to privacy on Art. 26(1) and provides that the law will lay down effective warranties against abusive, or contrary to human dignity, gathering or use of information relating to people (Art. 26(2). The Constitution individualizes the right to protection of digitalized personal data in Art. 35. On the other hand, Art. 37 enshrines *freedom of expression and information*, including the right to inform, to get information, and to be informed, without barriers or discrimination. All these rights can be seen as expressions of a human being's dignity[3].

The European Convention for the Protection of Human Rights protects the right to respect of private and family life (Art. 8) and the freedom of expression (Art. 10). The freedom of the press and the right to information are concretizations of that freedom, among others. It seems that the case law of the European Court for Human Rights is not entirely clear on the balancing these rights[4], depending on the particularities of the case which of the rights shall prevail[5].

At the EU level, the right to protection of personal data is enshrined in the Treaty on the Functioning of the European Union (Art. 16(1)) and in the Charter of Fundamental Rights of the European Union. This Charter not only protects the right to the respect of the private and family life (Art. 7), but also individualizes the right to personal data protection in Art. 8. This article provides, namely, that personal 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 (2).

Freedom of expression and information is also enshrined in the Charter (Art. 11).

The limitations to fundamental rights recognized by the Charter have to respect the principle of proportionality (Art. 52(1)): "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

The EU deemed necessary the harmonization of the Member States laws on personal data protection through the Directive 95/46/EC which was transposed to

[3] *Vid.* J. Miranda, *Direitos Fundamentais*, 2nd ed., Coimbra, Almedina, 2017, pp. 233–234.

[4] *Vid.* A. Fomperosa Rivero, "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality", *LSN Cyberspace Law eJournal*, vol. 22, nº 19, 2017 (available in SSRN), 22.

[5] *Vid.* S. Kulk and F. Borgesius, "Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal*, vol. 4, nº 13, 2017 (available in SSRN), 7 ss.

the Portuguese legal order by the *Lei da Proteção de Dados Pessoais* (Lei no 67/98, of 26/10).

This Directive has just approximated the laws of the Member States and, therefore, in Art. 4(1) there is a rule on the spatial scope of application of each Member State's transposition legislation[6], which was transposed to the Art. 4(3) of the *Lei de Proteção de Dados Pessoais* in terms that do not entirely correspond to the Directive's provision, but should be understood in the same sense according to an interpretation in conformity with the Directive[7].

The *ad hoc* connection rules provided in this statute resulted in the application of its material rules to matters concerning foreigners' rights of personality subjected, by the general conflicts law, to a foreign law, as referred below (III). These material rules were, therefore, susceptible of overriding application[8].

The Reglamento (EU) no 2016/679, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (*General Data Protection Regulation*, hereinafter referred to as GDPR) laid down a developed body of uniform material rules on personal data protection.

The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (Art. 2(1)). Some processing of personal data is excluded, namely that which is performed by a natural person in the course of a purely personal or household activity ((2)(c))[9].

---

[6] "1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."

[7] Art. 4 contains a paragraph 4 stating that the "act applies to video surveillance and other means of collection, processing and disclosure of sounds and images which allow the identification of persons whenever the controller is domiciled or seated in Portugal or uses a provider of computer and telematic networks established in the Portuguese territory."

[8] On the notion of rule susceptible of overriding application, *vid.* L. de Lima Pinheiro, *Direito Internacional Privado*, vol. I, *Introdução e Direito de Conflitos. Parte Geral*, 3rd ed., Coimbra, Almedina, pp. 270 ss.

[9] According to Recital no 18, personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such

Thus, the GDPR covers, namely, the processing of personal data by providers of goods and services on the internet.

The objectives of the GDPR are not only the protection of personal data of natural persons, but also to assure the free movement of this data within the Union (Art. 1)[10].

Art. 2(4) provides that the GDPR does not prejudice the application of Directive 2000/31/EC (*Directive on Electronic* Commerce), in particular its rules limiting the liability rules of intermediary service providers in the cases of mere conduit, caching and hosting and providing that there is no general obligation to monitor. This, however, does not mean that the GDPR rules are not applicable to the personal data protection in the context of the information society services, since that Directive safeguards the full application of the European legislation on personal data protection to the information society services (Recital no 14) and excludes from its scope of application questions relating to information society covered by that legislation (Art. 1(5)(b))[11].

In contrast, the operation of the domestic choice of law rule on torts is limited by the interpretation made by the ECJ on the case *eDate Advertising,* since it seems that the matter is covered by the coordinated field (Art. 2(h)(i))[12].

Among the *definitions provided by Art. 4* shall be stressed those of "personal data", mentioned above, "processing", "consent" and, below (II), "main establishment".

'Processing' means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (2).

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a

activities. However, the GDPR applies to controllers or processors which provide the means for processing personal data for such personal or household activities.

[10] Recital no 2 connects those objectives with the more general objective of contributing to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well–being of natural persons.

[11] For a different view, *vid.* D. Keller, "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation", *LSN Cyberspace Law eJournal*, vol. 22, nº 19, 2017 (available in SSRN), 66 ss.

[12] *Vid.* also P.A. de Miguel Asensio, "Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea", *Revista Española de Derecho Internacional*, 2017, pp. 75–108, esp. p. 106.

statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (11). This definition makes clear that the notion of consent relevant to the GDPR is autonomous and does not depend on the law governing the contract[13].

In the famous case *Google* (2014)[14], the ECJ held that Art. 2(b) and (d) of Directive 95/46/EC are to be interpreted as meaning that, first, the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) when that information contains personal data and, second, that the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d).

In the case *Wirtschaftsakademie Schleswig–Holstein* (2018)[15], the same court interpreted Art. 2(d) of the same Directive as meaning that the concept of 'controller' within the meaning of that provision encompasses the administrator of a fan page hosted on *Facebook*.

The GDPR also lays down a *regime of special material law on the transfer of data to third countries and to international organizations*.

Furthermore, the GDPR contains *many references to the law of the Member States*, which are in some cases unified choice of law rules, *some rules on jurisdiction* and one rule limiting the recognition of judgments and of administrative decisions of third countries.

The GDPR repealed the Directive 95/46/CE with effect as from 25 May 2018[16].

The European legislator considered that having in mind the fundamental right to personal data protection and the impact on this matter of the rapid technological developments and of globalization it was necessary to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union through an uniformization of the main material rules in this field[17].

---

[13] *Vid.* Ch. Kohler, "Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union", *Riv. dir. int. pr. proc.*, 2016, pp. 653–675, esp. pp. 663 ss.

[14] 13/5/2014 [ECLI:EU:C:2014:317].

[15] ECJ 5/6/2018 [ECLI:EU:C:2018:388].

[16] *Vid.* , also Art. 99(/2).

[17] *Cf.* Recitals nos 1, 6 and 10. The GDPR starts by reminding, in its Recital no 1, that the protection of natural persons in relation to the processing of personal data is a fundamental right. Recital no 6 points out the impact of the rapid technological developments and globalization in the field of personal data protection:

– the significant increase of personal data collection and sharing;

This means that now it is not only at stake the approximation of legislations, in terms that do not avoid the determination of the applicable national law, but the laying down of a uniform European regime. This uniformity implies that the same rules become applicable to domestic relationships and to transnational relationships, in contraposition to a mere unification of the regime applicable to transnational relationships.

With this achievement, *the problems of determination of the applicable law are not suppressed*. These problems are raised mainly at three levels: first, *the determination of the spatial scope of application of the GDPR*. (I), second, *the determination of the applicable law when the GDPR refers to the law of the Member States* (II), and third, *the determination of the national law applicable to issues that the GDPR does not govern* (III), not even by reference, such as most of the issues relating to torts resulting from the breach of the GDPR provisions.

The subject–matter of this essay covers these three problems. The aim, however, is just a first approach to this subject, since it comprises very wide, complex and controversial issues, which, in some cases, only began being studied very recently.

Outside the scope of this essay is the issue of the limits set by Public International Law as to the States' jurisdiction to prescribe, adjudicate, and enforce, without prejudice to the occasional allusions raised by certain legislative or judicial solutions.

II. Spatial scope of application of the GDPR

Regarding the spatial scope of application, Art. 3(1) starts providing that the GDPR 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.

The main issues raised by the interpretation of this provision concern the meaning of the expression "context of activities" and of the term "establishment".

– the use of personal data on an unprecedented scale in the pursuance of the activities of private companies and public authorities;

– the increasing availability of personal information publicly and globally.

The same Recital states that new technologies should facilitate the free flow of personal data within the Union and the transfer to third countries and international organizations, while ensuring a high level of protection of personal data.

According to Recital no 10, in order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States.

These issues were also raised in relation to Directive 95/46/EC and were the object of judgments by the ECJ, namely in the cases *Google*, *Weltimmo*, *Verein für Konsumenteninformation*, and *Wirtschaftsakademie Schleswig–Holstein*.

According to Recital no 22, the *establishment* implies the effective and real exercise of activity through stable arrangements and the legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

The reach of the statement that processing can de deemed as included in the context of the activities of an establishment located in the Union, regardless of whether the processing takes place in the Union or not, is illustrated by the judgment given in the aforementioned case *Google* on the right to erasure[18].

According to the opinion that was issued by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, established in terms of Art. 29 of the Directive, the notion "context of activities" implies that is applicable the law of the Member State where an establishment of the controller is involved in activities relating to data processing[19]. The ECJ, however, held that it was enough that *Google* had a subsidiary that carried out the *Google* group's advertising in Spain, but did not process the data, for the application of the Spanish rules transposing the Directive and condemned the *Google Spain* and the *Google Inc* to erase the personal data of a Spanish national in the results of the search engine[20].

[18] 13/5/2014 [ECLI:EU:C:2014:317].

[19] Opinion no 8/2010, 12–14. Afterwards the Working Party updated the Opinion taking into account the ECJ judgment. Se also the critique of M. Brkan, "Data Protection and European Private International Law", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal*, vol. 2, nº 43, 2015 (available in SSRN), 32.

[10] In this case, the ECJ faced issues related to the claim of a Spanish national, domiciled in Spain, against a Spanish publisher of a newspaper, *Google Spain*, and *Google Inc.*, based on the fact that when an internet user entered that person's name in the search engine of the Google group he would obtain links to two pages of the newspaper, on which an announcement for a real–estate auction connected with attachment proceedings for the recovery of social security debts, which mentioned that person's name. The person requested that *Google Spain* or *Google Inc.* remove or conceal his personal data so that they ceased to be included in the search results and no longer appeared in the links to the newspaper.

The ECJ interpreted Art. 4(1)(a) of Directive 95/46 as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.

Google Spain and *Google Inc.* had argued that the processing of personal data at issue in the main proceedings was carried out exclusively by *Google Inc.*, which operates Google Search without any intervention on the part of *Google Spain* and that the latter's activity is limited to providing support to the *Google group's* advertising activity which is separate from its search engine service.

The ECJ countered that results in particular from Recitals 18 and 20 in the preamble to Directive 95/46 and Article 4 thereof that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by

In the case *Wirtschaftsakademie Schleswig–Holstein* (2018)[21], the ECJ reaffirmed, regarding *Facebook*, the applicability of the law of the Member–State in which an establishment is situated that carries out an advertising activity even if personal data processing is made by establishments situated in a third State and in another Member State[22].

In my view, the compatibility of this solution with the limits set by Public International Law to a States' jurisdiction to prescribe and adjudicate, when it is not provided that the data subject shall be national or resident in that State, is doubtful.

On the other hand, results from the ruling on the case *Verein für Konsumenteninformation* that the fact that the undertaking responsible for the data processing does not have a branch or subsidiary in a Member State does not preclude it from having an establishment, but such an establishment cannot exist merely because the undertaking's website is accessible there[23].

---

prescribing a particularly broad territorial scope, and that, in this light, it is sufficient for the applicability of the law of a Member State that the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed (nos. 54 and 56).

According to G. van Calster, "Regulating the Internet. Prescriptive and Jurisdictional Boundaries to the EU's 'Right to Be Forgotten", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal*, vol. 2, nº 64, 2015 (available in SSRN), 24, referring to Ryngaert for the same view, the ECJ's judgment was technically based on the effects criterion to justify its jurisdiction regarding the relationship. Strictly, however, the issue concerns no only the jurisdiction to adjudicate and the jurisdiction to enforce, since itthe spatial scope of application of the Directive's regime was at stake and, therefore, an issue of the EU's jurisdiction to prescribe. Calster, *loc. cit.*, 25 ss, stresses that the jurisdiction to prescribe and to adjudicate is not necessarily followed by the jurisdiction to enforce and the ECJ has no jurisdiction to enforce regarding the site *Google.com*. Nevertheless, the jurisdiction to enforce concerns the power to carry out acts of material coercion. This power, even in the internet's context, is in principle confined to the territory of the forum State *(cf. Tallinn Manual 2.0 International Group of Experts and Other Participants*, General Editor Michael Schmitt, Cambridge, Cambridge University Press, 2017, *Rule* 11). Thus, if the Directive could be applicable and if there was a significant relationship with the EU, the court of a Member State may sentence the controlling corporation *Google* to remove certain data, but it can not carry out acts of material coercion regarding that controlling corporation. For a different view, *vid.* D. Nadeem, "Territorial Limits to the European Union's Right to be Forgotten: How the CNIL Ignores Jurisdictional Basics in Its March 10, 2016 Decision Against Google", *Creighton Int'l & Comp. L.J.*. 8 2017, pp. 182–199, esp. 191 ss and D. Nunziato, "The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten", *LSN Cyberspace Law eJournal*, vol. 23, nº 49, 2018 (available in SSRN), no 4.

[21] ECJ 5/6/2018 [ECLI:EU:C:2018:388].

[22] Nos 57 ss. In the same ruling, the ECJ held that the supervisory authority of a Member State is competent to assess, independently of the supervisory authority of the other Member State, the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene (no 74).

[23] ECJ 28/7/2016 [ECLI:EU:C:2016:612], no 76. Therefore,both the degree of stability of the arrangements and the effective exercise of activities in the Member State in question must be assessed (no 77, reaffirming the judgment in the case *Weltimmo*, ECJ 1/10/2015 [EU:C:2015:639], no 29). In regards

According to Art. 3(2), the GDPR *also 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, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behavior as far as their behavior takes place within the Union.

In this respect, Recital no 2, reinforced by Recital no 14, states that the "principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data".

There is a divergence between the different linguistic versions of Art. 3(2). While the Portuguese and Spanish versions refer to data subjects resident in the Union ["titulares residentes no território da União", "*interesados que residan en la Unión*"], the English, French, German and Italian versions refer to data subjects who are in the Union ["*who are in the Union*", "*personnes concernées qui se trouvent sur le territoire de l'Union*","*betroffenen Personen, die sich in der Union befinden*", "*interessati che si trovano nell'Unione*"]. Keeping in mind that the Regulation's Proposal in these latter versions referred to the residence, and that this reference was removed, and Recital no 14, it must be concluded that it is enough that the data subjects are in the territory of the Union at the moment in which the goods or services are offered or in which the behavior is monitored. This does not assure a significant relationship with the Union[24].

To extend the scope of application of the GDPR to cases in which neither the controller nor the processor is established in the Union nor the data subject is national or resident in the Union is, however, a solution of doubtful compatibility

to the question of whether the processing of personal data concerned is carried out "in the context of the activities", within the meaning of Art. 4(1)(a) of Directive 95/46, the ECJ also reaffirmed the judgment in the case *Weltimmo* (no 35), pointing out that that provision requires the processing of personal data in question to be carried out not 'by' the establishment concerned itself but only 'in the context of the activities' of the establishment (no 78). In the same ruling, it was held that Art. 4(1)(a) of Directive 95/46 must be interpreted as meaning that the processing of personal data carried out by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities, if it is shown that the undertaking carries out the data processing in question in the context of the activities of an establishment situated in that Member State. This is the Member State in whose territory the establishment is situated (no 74). Furthermore, the ECJ reaffirms the understanding, adopted in the case *Weltimmo*, that the concept of "establishment" within the meaning of Art. 4(1)(a) of Directive 95/46 extends to any real and effective activity, even a minimal one, exercised through stable arrangements (no 75).

[24] For a different view, of P.A. de Miguel Asensio, "Competencia y Derecho aplicable…", *loc. cit.*, 84–85.

with the limits set by Public International Law to the States' jurisdiction to prescribe. *The pursuance of the right to protection of personal data shall be based upon a significant relationship with the Union*.

In any case, it should be pointed out that the GDPR only applies to processing carried out by an entity non–established in the Union when the data subject is in the territory of the Union and one of the two above mentioned additional pre–requisites is fulfilled.

According to Recital no 23, in order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to the Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment. In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.

This understanding is close to the targeting criterion as developed by the ECJ's case law regarding jurisdiction on consumer contracts matters, namely the judgment given in the cases *Peter Pammer and Hotel Alpenhof* concerning Art. 15(1)(c) of Brussels I Regulation[25].

There are, however, differences, namely because the special regime of jurisdiction on consumer contracts matters, as well as the special choice of law rule on the law applicable to consumer contracts provided in the Rome I Regulation, presuppose the conclusion of a contract, which is not the case of the GDPR[26].

[25] *Cf.* ECJ 7/12/2010, in the cases *Peter Pammer* and *Hotel Alpenhof* [*in* http://curia.europa.eu]. *Vid.* also D. Cooper y C. Kuner, "Data Protection Law and International Dispute Resolution", *Recueil des Cours*, t. 382, 2015, pp. 9–174, esp. pp. 123–124.

[26] As remarked by P.A. de Miguel Asensio, "Competencia y Derecho aplicable…", *loc. cit.*, p. 85.

Therefore, on one hand, for the GDPR application it is not enough that there is an offer of goods or services on an internet site which may be purchased by data subjects that are in the Union[27], it is necessary to demonstrate an intention to offer these goods or services to these data subjects. On the other hand, however, considerable uncertainty remains about the factors which may be deemed relevant to demonstrate that intention and about their weight[28].

According to Recital no 24, in order to determine whether a processing activity can be considered to monitor the behavior of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes

M. Brkan remarks, in respect to the Regulation's Proposal, that interpretation elements are not conclusive in the meaning of this provision: a strict interpretation, that only covers the enterprises established in third countries that process information for economic purposes (such as *Google* and *Facebook*), or a broad interpretation, that would also cover data processing by public authorities, such as the NSA[29].

Regarding this issue, it should be pointed out that the GDPR excludes its applicability to data processing carried out in the course of an activity which falls outside the scope of Union law (Art. 2(2)(a)) or by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Art. 2(2)(d)).

This condition of applicability of the GDPR seems to have mainly in view the cases in which the placement of files and computer programs on the user's

[27] As resulted from the interpretation of the Regulation's Proposal advanced by M. Brkan, "Data Protection…", *loc. cit.*, p. 35.

[28] Art. 1(6) of Regulation on Geo–Blocking (Reglamento (EU) 2018/302) provides that "where a trader, acting in accordance with Articles 3, 4 and 5 of this Regulation, does not block or limit consumers' access to an online interface, does not redirect consumers to a version of an online interface based on their nationality or place of residence that is different from the online interface to which the consumers first sought access, does not apply different general conditions of access when selling goods or providing services in situations laid down in this Regulation, or accepts payment instruments issued in another Member State on a non–discriminatory basis, that trader shall not be, on those grounds alone, considered to be directing activities to the Member State where the consumer has the habitual residence or domicile. Nor shall that trader, on those grounds alone, be considered to be directing activities to the Member State of the consumer's habitual residence or domicile, where the trader provides information and assistance to the consumer after the conclusion of a contract that has resulted from the trader's compliance with this Regulation".

[29] M. Brkan, "Data Protection…", *loc. cit.*, pp. 35–36.

appliance providing access to information (such as cookies) does not occur in the context of the offering of goods and services[30].

The cases in which the application of the GDPR is justified albeit the processing is not carried out in the territory of a Member State are, in principle, covered by the connecting factors of Art. 3(2) and, therefore, the broad interpretation of the "context of activities" of an establishment situated in a Member State adopted by the ECJ in the *Google case* should not be maintained.

A certain restraint in the exercise of the States' jurisdiction to prescribe relating to internet is important, since laws with a very wide spatial scope of application easily conflict with the laws of other States, raising problems of conflict of duties for their addressees and of recognition in other States of judgments based upon these laws[31].

Art. 3(3) adds that the GDPR applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of Public International Law.

The law of a Member State applies by virtue of Public International Law for example in a Member State's diplomatic mission or consular post (Recital no 25).

The GDPR gave up the connection criterion laid down on Art. 4(1)(c) of Directive 95/46/EC – location of equipment for personal data processing, automated or otherwise, in the territory of a Member State, unless such equipment is used only for purposes of transit through the territory of the Community –, because it was considered that this criterion led to an excessive scope of application of the European regime, including cases which do not have a significant relationship with the EU[32].

III. Determination of the applicable law when the GDPR refers to the law of the Member States

The GDPR contains many references to the law of the Member States, which would be irksome to enumerate here.

In a considerable number of cases, *these references are made by a choice of law rule pointing to the law of the State to which the controller or the processor are subject*.

[30] For this view, P.A. de Miguel Asensio, "Competencia y Derecho aplicable…", *loc. cit.*, 86. *Vid.* further C. Keller, "The Right Tools…", *loc. cit.*, p. 58.

[31] *Vid.* , the remarks of C. Kuner, "The Internet and the Global Reach of EU Law", *LSN Cyberspace Law eJournal*, vol. 22, nº 15, 2017 (available in SSRN), 32–33.

[32] *Vid.* P.A. de Miguel Asensio, "Competencia y Derecho aplicable…", *loc. cit.*, pp. 80–81.

This is the case of Art. 6(3), 14(5)(c), 17(1)(e) and (3)(b), 22(2)(b), 23(1), 26(1), 49(1)(d) and (4), and 85(2) (coordinated with Recital no 153).

The controller or the processor are certainly subject to the law of the State where they are established. Nevertheless, doubts arise when they have a plurality of establishments in different Member States. Art. 4(16) provides a definition of main establishment which is at least relevant to determine the lead supervisory authority. According to this definition "as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment"[33].

When the data is processed by a secondary establishment the entity should be deemed subject to the law of the Member State of this establishment or to the law of the Member State of the main establishment?

In favor of the competence of the law of the Member State in which the establishment processing the data is situated, the criterion in principle relevant for the determination of the spatial scope of application of the GDPR (Art. 3(1)) as well as the judgment in the case *Weltimmo*[34], concerning the law applicable to data protection according to the Directive 95/46/EC may be invoked . For the law of the State of the main establishment, it may argued that this establishment is relevant in the determination of the lead supervisory authority for the cross–border processing. The clarification of this issue by the ECJ will be welcome.

In some cases, *different connection criteria* are laid down.

Thus, concerning the operation of members of the staff of the supervisory authority of one Member state in another Member State, the GDPR provides for the application of the law of the Member State in which they operate, including the liability for damages caused during their operations (Art. 62(3) to (5)).

On the other hand, personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with

[33] Furthermore, "as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation".

[34] *Supra cit.*, nos 24 ss.

Union or Member State law to which the public authority or body is subject (Art. 86).

In other cases, *the reference does not provide a connecting factor*. In these cases, the determination of the scope of application of the law of the Member Sates is subject to their domestic law. They can do it through a mere unilateral and *ad hoc* choice of law rule, i.e., which only defines the spatial scope of application of the substantive rules in question, or, in principle, to adopt bilateral choice of law rules that refer either to the forum law or to the law of other Member States. The reason why the GDPR does not define the relevant connecting factor in these cases is not entirely clear. Anyway, it seems that this option does not preclude that the Member States resort to the criterion of the controller or the processor's establishment. In favor of resorting to this criterion in matters concerning the rights and duties of these entities, the systematic coherence with the solution favored by the GDPR may be invoked. For the contrary view, it can be argued that a law with a special close relationship with the data subjects should be applicable, since the GDPR has as first objective the protection of their rights. This issue will be addressed in the subsequent point (III).

On the other hand, *the location of the electronic data is problematic and does not seem to be an appropriate connection factor for Private International Law*, on the determination of the law applicable to personal data protection[35].

Personal data is information, and the information is a spiritual creation and not a tangible thing. Data, as such, does not have a physical location; what has a physical location are the devices where the data are stored. Electronic personal data can be stored in different devices, namely servers and hard drives of personal computers. The present trend regarding personal data processed by enterprises is storage under provision of services of cloud computing. Not only the place of storage of the files containing these data can result from mere technical options of the enterprises that provide services on the internet, without any other connection

[35] It is more controversial whether it is a factor of connection appropriate for the delimitation of States' jurisdiction under Public International Law. *Vid.* , *Tallinn Manual 2.0 International Group of Experts and Other Participants*, Rule 1, no 4, and Rule 2, no 11; *Microsoft* v. *United States*, decided on appeal by the *United States Court of Appeals for the Second Circuit* (2016) (available in https://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf?ts=1468508412); Keane WOODS – "Against Data Exceptionalism", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal*, vol. 3, nº 16, 2016 (available in SSRN), 734 and seq. and 754 ss.; T. Christakis, "Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)", *LSN Cyberspace Law eJournal*, vol. 23, nº 2, 2018 (available in SSRN), 24 ss, but putting forward solutions which are not based upon the place of data's storage nor upon the place of access to the data; and S. Watts y T. Richard, "Baseline Territorial Sovereignty and Cyberspass", *LSN Public International Law: Foreign Relations & Policy Law eJournal*, vol. 5, nº 18, 2018 and *LSN Cyberspace Law eJournal*, vol. 23, nº 33, 2018 (available in SSRN), 851 ss.

with the enterprises or the data subjects, but also segments of the same file can be stored in servers located in different States.

To finalize this point, it should be stressed that one of those references to the law of the Member States is contained in Art. 85, providing that *Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information as enshrined in Art. 11 of the Charter*, including processing for journalistic purposes and the purposes of academic, artistic or literary expression (no 1 and Recital no 153)[36].

Therefore, the balancing of the right to protection of personal data with the right to freedom of expression and information depend to a large extent on the laws of the Member States, raising the issue of the substantive solutions that should de adopted and of their spatial scope of application.

With respect to Art. 9 of Directive 95/46/EC, which was the normative precedent of that provision, the ECJ held, in the case *Satakunnan Markkinapörssi* and *Satamedia*, that in order to achieve a balance between the two fundamental rights the derogations and limitations in relation to the protection of data must apply only in so far as is strictly necessary[37].

The initial Proposal of the Rome II Regulation on the Law Applicable to Non–Contractual Obligations provided, in Art. 6(1), that the "law applicable to a non–contractual obligation arising out of a violation of privacy or rights relating to the personality shall be the law of the forum where the application of the law designated by Article 3 would be contrary to the fundamental principles of the forum as regards freedom of expression and information".

Thus, the general rule of the law of the place of the damage would apply to the violation of privacy, but the forum law would replace the foreign governing law when this would be required by fundamental principles of the forum law as regards freedom of expression and of information. This rule was excluded from the final version of the Regulation due to irreconcilable divergences with the European Parliament.

Art. 85 of GDPR does not impose the application of the forum law to this balancing, as provided in that Proposal. On the contrary, Recital no 153 points to the prevalence of the law of the Member State to which the controller is subject

[36] This should apply in particular to the processing of personal data in the audiovisual field and in news archives and press libraries (Recital no 153). In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom, such as journalism, broadly (Recital no 153).

[37] ECJ 16/12/2008 [ECLI:EU:C:2008:727], no 56. For a comparison of the solutions adopted by the Member States in the transposition of this provision, *vid.* D. Erdos, "European Union Data Protection Law and Media Expression: Fundamentally Off Balance", *Int. Comp. L. Q.*, vol. 65, 2016, pp. 139–184, esp. pp. 50 ss.

regarding the derogations and exemptions relating to processing of personal data solely for journalistic purposes, or for the purposes of academic, artistic or literary expression (provided in Art. 85(2)).

In any case, it seems defensible that a balancing of fundamental rights being at stake, the forum law is applied whenever the relationship has a significant connection with the forum State or with other State (Member State or third State) in which similar fundamental conceptions are in force.

To this purpose, the adoption of a special provision addressing this issue should be preferred, which defines the relevant connections with the forum State, considering the interpretation of the constitutional rules in question and the methods and criteria of balancing with respect to the collision of fundamental rights.

IV. Determination of the national law applicable to issues that the GDPR does not govern

The determination of the law applicable to the issues of private law which the GDPR does not govern must be based on the general choice of law rules.

In the Portuguese legal order, Art. 27(1) of the Civil Code provides that the "personal law is also applicable to the rights of personality, in what concerns their existence and protection and to the restrictions imposed to their exercise".

The personal law is, in principle, the law of the nationality (Art. 31(1) of the Civil Code).

Therefore, the granting of the rights, their content and the restrictions imposed to their exercise are governed by the personal law. Regarding the restrictions imposed to the exercise of the right, the personal law applies both to legal restrictions and to the validity and effects of the voluntary limitations.

Although according to Art. 27(1) personal law governs the protection of the right, it shall be understood that the general remedy – civil liability for infringement of personality rights – is subject to the law applicable to torts[38].

Regarding specific remedies, it is necessary to consider the provision contained in para. 2 of the same Article: "The foreigner or stateless does not enjoy, however, any remedy which is not recognized by Portuguese law". This provision raises

[38] *Cf.* J. Baptista Machado, *Lições de Direito Internacional Privado*, 2nd ed., Coimbra, Almedina, 1982, p. 343. On the choice of law rules governing the violation of the *right of publicity*, *vid.* E. Dias Oliveira, "A relevância do *right of publicity* no âmbito da propriedade intelectual", *Estudos de Direito Intelectual em Homenagem ao Prof. Doutor José de Oliveira Ascensão*, Coimbra, Almedina, 2015, pp. 228 ss y pp. 209–232.

some interpretation doubts. According to the most common view, it can only be enforced in Portuguese courts' remedies (preventive or repressive) that are allowed both by the foreign personal law and by Portuguese law[39]. This amounts to a case of cumulative connection. It has also been sustained that this is a rule of Foreigners Law[40], leading to the same practical result.

These views do not take into account the delimitation between procedural issues, which are necessarily subject to the *lex fori*, and substantive issues. The provision can be understood in conformity with the applicability of the Portuguese law, as *lex fori*, in procedural matters[41]. In this line, the foreign personal law decides on the claims that the interested person may enforce, the Portuguese law on the procedural means through which these claims may be enforced. The laws at stake are, in principle, of distributive, and not cumulative application, albeit, in practical terms, it can be that certain claims based upon the foreign personal law do not find an appropriate procedural mean to be enforced in Portuguese courts.

This reasoning does not apply to modes of self protection. These modes must be allowed by the foreign personal law; when they imply the use of coercive means they have to be permitted also by Portuguese law, since the use of coercive means depends on the local law[42].

On the other hand, regarding specific remedies for the infringement of personality rights which shall be deemed covered by the Rome II Regulation in spite of the exclusion laid down by Art. 1.º/2/g[43], it should be born in mind the provision contained in Art. 15(d) of this Regulation that subjects"the measures which a court may take to prevent or terminate injury or damage", "within the limits of powers conferred on the court by its procedural law" to the law governing the non–contractual obligation.

Therefore, it seems that the specific remedies will depend, in this case, on the law designated by the choice of law rules of the Regulation, within the limits set by the competence of the *lex fori* in procedural matters. As below stated, it should be understood that the Rome II Regulation does not cover the liability for infringement of rights granted by the GDPR to the data subjects.

---

[39] J. Baptista Machado, *Lições…*, *op. cit.*, p. 343 and R. Capelo de Sousa, *O Direito Geral de Personalidade*, Coimbra, Editora, 1995, p. 504.

[40] A. Marques dos Santos, *Direito Internacional Privado. Sumários*, 2nd ed., Lisbon, AAFDL, 1987, pp. 246 ss.

[41] *Vid.* L. de Lima Pinheiro, *Direito Internacional Privado*, vol. II, *Direito de Conflitos. Parte Especial*, 4th ed., Coimbra, Almedina, 2015, § 52.

[42] Besides international treaty providing otherwise.

[43] *Vid.*, on this issue, L. Lima Pinheiro, *Direito Internacional Privado*, vol. II, *op. cit.*, pp. 474–475, with more references.

Although the personality principle points towards the application of personal law to the grant personality rights and to their content, the solution adopted by most systems subjects these issues to the law governing torts ([44]). In favor of this solution it argued, namely, the advantage of avoiding the *dépeçage* between the law governing the personality rights and the law governing the liability for their infringement; the effects *erga omnes* of the personality rights that demands the use of connecting factors that are easily cognoscible by all interested parties; and the possibility that the relationship involves a conflict of rights between the tortfeasor and the victim, which requires a neutral and foreseeable connection for both parties.

Against this solution it is objected that personality rights are not only relevant when an infringement occurs, but also in cases where it is only necessary to demonstrate their existence, for example, to know if there is a personality right that can be the object of a contract[45]. To this objection, however, it can be opposed that independently of being in question an infringement, it is possible, in principle, to consider the law of the country in which the damage would occur, if the right existed and was violated. This means a hypothetical reasoning. If that law grants the right, all the interested parties know that their conduct shall respect that right or incur in liability for the damages caused by its infringement and be object of preventive or repressive remedies. If that law does not grant the right, the interested parties know that their conduct is not conditioned by it.

For sure, this solution should be preferred to any cumulative connection that makes the granting and the content of the right simultaneously dependent on the personal law and the forum law or the law governing torts[46], which would weaken the protection of personality rights.

Within the scope of application of the GDPR, the granting of rights to the protection of personality rights, their content and the restrictions imposed to their exercise are, in principle, governed by this Regulation, even if the personal law of the data subject is the law of a third State, since it is directly applicable to these rights. This means that *the choice of law rule of Art. 27(1) of the Civil Code only can play a role regarding personal data protection outside the scope of application*

[44] *Vid.*, namely, *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, Einführungsgesetz zum Bürgerlichen Gesetzbuche, Art 38 – 42 EGBGB, Neubearbeitung 2001*/Von Hoffmann, Berlin, Sellier– De Gruyter, Art. 40 EGBGB no 54; and *Münchener Kommentar zum Bürgerlichen Gesetzbuch*/Junker, vol. X, 6th ed., Munich, C. H. Beck, 2015, EGBGB Art. 40 no 83.

[45] *Vid.* E. Dias Oliveira, *Da Responsabilidade Civil Extracontratual por Violação de Direitos de Personalidade em Direito Internacional Privado*, Coimbra, Almedina, 2011, p. 292.

[46] *Ibid.*, pp. 295 ss, defending that Art. 27 of the Civil Code, understood in the light of the "principle of protection of reliance", shall be interpreted in the sense that the restriction contained in its para. 2 does not refer only to the remedies but also to the rights protected, when there is a contact between the relationship and the Portuguese legal order.

of the GDPR or, eventually, regarding the issues that the GDPR subjects to the law of the Member States without defining the relevant connecting factor.

Regarding these issues, we have seen that systematic coherence may point towards the applicability of the law of the State to which the controller or the processor are subject (II), while the main objective of the GDPR, which is the protection of the data subjects, offers an argument in favor of the application of the law of the States with most significant relationship with the data subject. *A differentiation seems unavoidable, according to the interests at stake.*

Where there are public interests directly at stake, it should be expected that the Member States pursuing these interests delimitate the scope of application of the substantive rules protecting these interests through a unilateral choice of law rules.

Issues concerning the constitution, functioning and activities of the supervisory authorities should, in principle, be governed by the law of the Member State to which the authority belongs.

In other cases, it seems to me that, in principle, according to the principle of personality, the application of the law of a State which as a significant relationship with the data subject should be preferred. Cases should be excepted in which private interests that do not interfere directly with interests of the data subject, namely interests of the controller and/or of the processor. are at stake.

In the determination of that law, it is also important to keep in mind the convenience of applying the same law which governs torts resulting from the infringement of the data subject's rights and of a convergence between the applicable law and the forum with jurisdiction.

In relation to Art. 5(3) of Brussels I Regulation (jurisdiction on matters relating to tort, delict and quasi–delict), the ECJ held in the case *eDate Advertising* (2011)[47] that the criterion of the place of damage caused to the holder of a personality right raised difficulties when the infringement results from a content inserted in the internet, since this content is available on a world–wide basis and, therefore, it must be adapted. On this basis, the court held that the jurisdiction can be grounded on victim's center of interests, which corresponds, in principal, to his habitual residence[48].

The ECJ added that a person may also have the center of his interests in a Member State in which he does not habitually reside, in so far as other factors, such as the pursuit of a professional activity, may establish the existence of a particularly close link with that State[49].

[47] 25/10/2011 [*in www.curia.europa.eu*].
[48] Nos 47–49.
[49] No 49.

As I had previously advocated, although a mechanical transposition of this solution to the determination of the law applicable to torts resulting from the infringement of personality rights through the internet should not be done, it is conceivable that an appropriate solution in this matter takes into consideration the victim's habitual residence and, more widely, his center of interests[50].

Furthermore, Art. 79(2) of GDPR provides that the data subjects may opt between bringing proceedings against the controller or the processor before the courts of the Member State in which the controller or processor has an establishment or in the courts of the Member State where the data subject has his or her habitual residence[51].

These considerations lead me to the conclusion that it is *the law of the State where the data subject has his center of interests that is in the best position to govern his rights in an internet context*. Outside the scope of application of the GDPR this solution only seems defensible *de iure condendo*. Within the scope of application of the GDPR, but concerning issues that it subjects to the law of the Member States without defining the relevant connecting factor, the necessity of avoiding an excessive segmentation of the relationships, through the application of the GDPR regime, of the personal law of the data subject and of the law governing torts, seems to justify a teleological reduction of Art. 27(1) of the Civil Code, and the filling of the gap resulting from it with this solution.

Regarding the issues that the GDPR does not govern, the law applicable to contracts, determined according to the Rome I Regulation, has a role to play regarding obligations freely assumed by the controller or processor towards the data subject[52].

It shall be remarked that when the contract is governed by the law of a third State according to the Rome I Regulation, the GDPR regime overrides that law, by its own effect, and not by operation of Art. 9(2) of the Rome I Regulation[53].

---

[50] *Vid.* convergent proposals referred by E. Dias Oliveira, "Algumas considerações sobre a responsabilidade civil extracontratual por violação de direitos de personalidade em Direito Internacional Privado", *Cuadernos de Derecho Transnacional*, nº 5, 2013, pp. 139–162, esp. pp. 147–148 nos. 34 and 35, and, for the different view of the author, *loc. cit.*, pp. 160 ss.

[51] *Vid.* also Recital no 145 and Art. 82(6). The forum of the habitual residence of the data subject is, however, excluded where the controller or processor is a public authority of a Member State acting in the exercise of its public powers (no 2 *in fine*).

[52] *Vid.* also Ch. Kohler, "Conflict of Law Issues…, *loc. cit.*, p. 671. Raising the doubt on this point, with reference to the above mentioned ECJ judgment in the case *Verein für Konsumenteninformation*, S. Corneloup, "De la loi applicable aux activités des entreprises de commerce électronique", *Rev. crit. dr. int. pr.*, 2017, pp. 112–122.

[53] For this view, however, Ch. Kohler, "Conflict of Law Issues…, *loc. cit.*, p. 661 and P.A. de Miguel Asensio, "Competencia y Derecho aplicable…", *loc. cit.*, p. 104. Regarding Directive 95/46/EC, *vid.* M. Brkan, "Data Protection…", *loc. cit.*, pp. 26 ss.

In practice, however, the most important issue are the torts resulting from the infringement of rights to the protection of personal data[54].

Art. 82 of GDPR contains some rules on the liability of the controller or processor towards any person who has suffered material or non–material damage as a result of an infringement of this Regulation.

These rules:

– recognize to any person who has suffered damages the right to receive compensation from the controller or processor;

– limit the liability of the processor to cases where it has not complied with obligations of the Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller;

– exempt from liability the controller or processor if it proves that it is not in any way responsible for the event giving rise to the damage;

– provide that where more than one controller or processor, or both a controller and a processor, are involved in the same processing each controller or processor shall be held liable for the entire damage.

Recital no 146 provides important guidelines for the interpretation of this article.

First, the concept of damage should be broadly interpreted in the light of the case–law of the ECJ in a manner which fully reflects the objectives of the GDPR.

Second, the provision does not prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law.

Third, processing that infringes the GDPR also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of the GDPR.

Fourth, data subjects should receive full and effective compensation for the damage they have suffered.

Last, although each of the controllers or processor involved in the same processing are held liable for the entire damage, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured.

[54] P.A. de Miguel Asensio, "Competencia y Derecho applicable...", *loc. cit.*, pp. 105–106, stresses the possibility of difficult problems of delimitation between the GDPR regime, which depends on an autonomous connection, and the law governing torts, regarding the responsibility for infringement of the GDPR rules.

The other issues of the liability of the controller or processor are governed by the law applicable to torts.

On the law applicable to torts, the *Rome II Regulation* is in force in the Portuguese legal order, but Article 1(2)(g) excludes the non–contractual obligations arising out of violations of privacy and rights relating to personality from its scope. Albeit this exclusion of the personality rights should be interpreted restrictively, considering the connection between personal data protection and privacy, as it seems that the exclusion covers the liability for infringement of rights to protection of personal data[55].

For this reason, one should resort to the domestic choice of law rule, provided in Art. 45 of the Civil Code.

Art. 45(1) of the Civil Code subjects the fault–based liability and no–fault liability "to the law of the State where occurred the main activity causing damage; in case of liability by omission, the law of the place where the tortfeasor should have acted is applicable"[56].

Nevertheless, by operation of para. 2 the law of the State where the injury occurred applies where it deems the tortfeasor liable, but not the law of the country where his activity occurred, provided that the tortfeasor should foresee the occurrence of a damage in that State, as consequence of his act or omission.

In the cases of infringement of the protection of personal data in the context of the internet, *which is the place of the activity causing damage*?

I believe that both the place where the personal data are processed and the place where the controller or processor access the internet[57] could be relevant as place

[55] As well as the violation of rules of protection of personal data that do not grant subjective rights. *Cf.* Ch. Kohler, "Conflict of Law Issues...", *loc. cit.*, pp. 673–674 and P.A. de Miguel Asensio, "Competencia y Derecho aplicable…", *loc. cit.*, pp. 105–106. For a different view, M. Brkan, "Data Protection…", *loc. cit.*, pp. 26 ss, with more references. P.A. de Miguel Asensio [*loc. cit.*] sustains that the interests at stake point towards the applicability of the law of the place where the interests or rights of the victim are injured, typically his habitual residence or "center of interests". See, with further development, *id.*, *Derecho Privado de Internet*, 5ª ed., Cizur Menor (Navarra), Civitas and Thomson Reuters, 2015, 217–218. The author invokes the parallelism with the jurisdiction rule of Art. 79(2) GDPR, but this parallelism would point more towards the alternative application of the law of the establishment of the controller (which is, in principle, the law of the place of the activity) and the law of the habitual residence of the data subject.

[56] *Vid.* , also Art. 16 of the Brussels Convention on Mutual Assistance in Criminal Matters Between States Marber of the EU (2000), regarding civil liability of the officials of a Member State who are in mission in another Member State.

[57] *Cf.* P. Mankowski, "Das Internet im Internationalen Vertrags– und Deliktsrecht", *RabelsZ*,. 63, 1999, pp. 203–294, esp. p. 257. *Cf.* J. Fawcett and P. Torremans, *Intellectual Property and Private International Law*, 2nd ed., Oxford, Oxford University Press, 2011, no 16.104, sustaining that defamation is committed in all the States where is downloaded the defamatory material, and *Dicey, Morris and Collins on the Conflict of Laws* – 15th ed. by Lord Collins of Mapesbury (general editor), A. Briggs, A. Dickinson, J. Harris, J. McClean, P. McEleavy, C. McLachlan e C. Morse, London, Sweet & Maxwell and Thompson

of the activity causing damage. Normally, they coincide. If this coincidence does occur, the place where the data is processed should be deemed the place of the main activity.

The determination of the places where the data are processed and where the tortfeasor accesses the net may raise great difficulties. These places can not be cognoscible by the data subjects or only be cognoscible at a prohibitive cost[58]. As a resort solution, Art. 45 may be interpreted in the sense that the law of the place of injury applies where it is not possible to determine the place of activity.

Furthermore, regarding torts perpetrated trough broadcasting, satellite transmission and computer network, the risk of manipulation of the connecting factor place of activity is particularly high. The operator can easily move the place of its activity to a particularly permissive State. The possibility of applying the law of the place of the injury where the law of the place of activity does not deem the tortfeasor liable does not annul this risk, because the law of the place of activity can subject the tortfeasor to a less strict liability regime than the law of the place of injury.

This aggravated risk of *fraus legis* could be prevented by a special provision according to which, in the case of tort committed through these means, the victim may opt between the application of the law of the place of activity and the application of the law of the habitual residence or seat of the tortfeasor.

A near solution was adopted by Art. 139(1) of the Swiss Private International Law Act which, concerning the claims grounded on infringement of personality rights through public communication means , grants to the victim a choice between the law of the State of the victim's habitual residence, provided that the tortfeasor could count with the occurrence of the result in this State, the law of the State of establishment or habitual residence of the tortfeasor, and the law of the State where the result of the infringement occurs, provided that the tortfeasor could count on the occurrence of the result in this State.

A second issue is *the determination of the place where the injury occurs*.

Regarding the infringement of personality rights through the insertion of content on the internet the injury can occur in all the places in which it is allowed the access to the net[59]. Although this multiplication of places of injury can be restricted, in certain cases, in function of the content of the personality right in question[60], it always potentially implies a segmentation of the applicable law

Reuters, 2012, no 35–119, understanding as place of commission the place where the material is downloaded or retrieved, at least if the claimant suffers damage to reputation in that place.

[58] *Vid.* proposals for the solution of this problem in P. Mankowski, "Das Internet…", *loc. cit.*, pp. 258 ss.

[59] *Ibíd.*, p. 269, with some exceptions.

[60] Thus, the defamation occurs only in the States in which the victim is known. In effect, the good name and reputation only can be harmed by the statement or disclosure of facts in a social circle in which the

which can lead to difficult resolution problems and does not take into consideration the principle of the closest relationship[61]. These considerations justify an adaptation of the conflictual solution, which, in the above–mentioned terms, can *to a certain extent* be inspired by the ECJ's case law on Art. 5(3) of the Brussels I Regulation (jurisdiction on matters relating to tort, delict and quasi–delict)[62] and on Art. 79(2) RGPD (jurisdiction for the proceedings concerning liability by the infringement of the rights granted by the GDPR to the data subject).

Therefore, the place where the data subject has his habitual residence or, more widely, his center of interests, shall be understood as the place of the injury.

Converging with Art. 4(3) of the Rome II Regulation, I believe that another deviation would be justified by the idea of respecting the interdependence of sets of rules, similar to the one provided in Art. 133(3) of the Swiss Private International Law Act and in Art. 41(2)(1) of the Introductory Act to German Civil Code, with the wording given in 1999[63]. According to this deviation, if between the tortfeasor and the victim there is a preexisting relationship, it will be the law applicable to this relationship which, in principle, will govern the tort.

---

concerned person is known. For a similar reason, the case of liability provided in Art. 484 of the Civil Code (defamation) only occurs when a fact is stated or disclosed in the social circle in which the concerned person lives or pursues his activity – *cf.* J. de M. Antunes Varela, *Das Obrigações em geral*, 10th ed., Coimbra, 2004, p. 549.

[61] *Vid.*, also P.A. de Miguel Asensio, "Competencia y Derecho aplicable…", *loc. cit.*, pp. 217–218.

[62] In the above–mentioned case *eDate Advertising* (TUE 25/10/2011 [in http://curia.europa.eu], no 52), the ECJ held that in the event of an alleged infringement of personality rights by means of content placed online on an internet website, the person who considers that his rights have been infringed has the option of bringing an action for liability, in respect of all the damage caused, either before the courts of the Member State in which the publisher of that content is established or before the courts of the Member State in which the center of his interests is based. That person may also, instead of an action for liability in respect of all the damage caused, bring his action before the courts of each Member State in the territory of which content placed online is or has been accessible. Those courts have jurisdiction only in respect of the damage caused in the territory of the Member State of the court seized.

[63] The provision of the German law includes this solution in an escape clause and extend it to the existence of a factual relationship between the interested parties. *Vid.* further J. Kropholler, *Internationales Privatrecht*, 6th ed., Tübingen, Mohr Siebeck, 2006, pp. 530 ss; the converging remarks of A. Ferrer Correia, *Direito Internacional Privado. Alguns problemas*, Coimbra, Almedina, 1981, pp. 105 ss; and A. De Sousa Gonçalves, *Da Responsabilidade Extracontratual em Direito Internacional Privado. A Mudança de Paradigma*, Coimbra, Almedina, 2013, pp. 410–411; and the works referred by R.M. Moura Ramos, *Da Lei Aplicável ao Contrato de Trabalho Internacional*, Coimbra, Almedina, 1991, 378 n. 19. *Vid.*, further D. Moura Vicente, *Da Responsabilidade Pré–Contratual em Direito Internacional Privado*, Coimbra, Almedina, 2001, pp. 498 ss, with developed bibliographic and comparative references, who accepts in a limited manner this deviation even *de iure constituto*, followed by E. Dias Oliveira, *Da Responsabilidade Civil Extracontratual…*, *op. cit.*, pp. 523–524.

Furthermore, in my view, the domestic choice of law rules should converge with the Rome II Regulation regarding the admissibility of choice by the parties of the law applicable to non–contractual obligations[64].

The above–mentioned regime is also applicable to torts committed by providers of services online, since the DL no 7/2004, of 7/1, interpreted in conformity with the *Directive on Electronic Commerce*, does not displace the choice of law rule of Art. 45 of the Civil Code[65]. Notwithstanding, it results from the understanding held by the ECJ, in the above–mentioned case *eDate Advertising* (2011), that the law referred to by Art. 45 of the Civil Code may not subject the providers established in a Member State to stricter requirements than those provided for by the substantive law in force in the Member State in which that service provider is established.

V. Final remarks

Without going into the controversy raised by some substantive solutions, it can be affirmed that the wide uniformization of the substantive law applicable to personal data protection in the EU is, in principle, justified. The spatial scope of application of the GDPR, however, seems too broad, not ensuring that there is always a significant relationship with the EU.

Art. 50 provides for the taking of appropriate steps for the international cooperation with third countries and international organizations that are of great importance:

– develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

– provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral,

[64] *Vid.* , also Art. 42 of the Introductory Act to the German Civil Code, with the wording given in 1999. In my view it is not defensible the admissibility of the choice of law before the law in force, as sustained by N.A. Pissarra, *O Dano Transnacional em Direito Internacional Privado. Alguns Problemas* (polycopied master dissertation), Lisbon, 2004, 153 ss. The legislator opted unequivocally, in Art. 45 of the Civil Code, for objective connecting factors and therefore it would be clearly against the legislative purpose to allow the conflictual freedom of choice in this matter.

[65] *Vid.* L. de Lima Pinheiro, *Direito Internacional Privado*, vol. II, *op. cit.*, § 65 D *in fine* and 68 *B in fine*. On this issue, before the ECJ judgment in the case *eDate Advertising*, *vid.* L. de Lima Pinheiro, "Direito aplicável à responsabilidade extracontratual na *Internet*", *Revista Faculdade de Direito da Universidade de Lisboa*, 42, 2001, pp. 825–834, esp. pp. 833–834; *id.*, "O Direito de Conflitos e as liberdades comunitárias de estabelecimento e de prestação de serviços", *Seminário sobre a Comunitarização do Direito Internacional Privado*, 79–109, Coimbra, Almedina, 2005, pp. 79-109 (=*in Estudos de Direito Internacional Privado*, pp. 357–387, Coimbra, Almedina, 2006) pp. 102 ss, with further references.

investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;

– engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; and

– promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

The importance of this international cooperation is evidenced by some very debated judgments not only relating to the international protection of personal data but also concerning the cross–border criminal investigation[66].

The internet, as a global reality, requires global regulation, which to a large extent can be provided by private organizations representative of the community of the internet stakeholders, but also requires, in several fields, as it is the case of personal data protection, a regulation by international conventions of universal scope[67].

Some steps have already been taken towards the international unification of the rules applicable to personal data protection, but with limited reach.

Thus, the Council of Europe adopted in 1981 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), of which all the Member States of the Council are parties, but that only obtained a very limited acceptance by other States. In 2001, a Protocol Regarding Supervisory Authorities and Transborder Data Flows was opened for signature, of which 36 of the 47 Member States of the Council are parties, including Portugal, and that also only obtained a very limited acceptance by other States. Aiming at the modernization of the Convention 108, namely to deal with challenges resulting from the use of new information and communication technologies, the Council of Europe recently adopted a new Protocol amending the Convention 108. The consolidated text resulting therefrom is called Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+).

---

[66] *Vid.* namely, T. Christakis, "Data, Extraterritoriality and International Solutions…", *loc. cit.*, pp. 35 ss.

[67] *Vid.* R. Weber (in collaboration with M. Grosz), *Shaping Internet Governance: Regulatory Challenges*, Zurich, Basel and Geneva, Springer, 2009, pp. 16–17; and L. de Lima Pinheiro, "Reflexões sobre a governação e a regulação da internet, com especial consideração da ICANN", *Estudos de Direito Intelectual em Homenagem ao Prof. Doutor José de Oliveira Ascensão*, Coimbra, Almedina, 2015, pp. 363–385, esp. pp. 371–372. Considering that the political viability of this international unification is highly doubtful, M. Brkan, "Data Protection…", *loc. cit.*, pp. 36–37. An international unification of the rules on jurisdiction and choice of law, suggested by the author, appear, however, less appropriate.

Besides the geographical limitation, these instruments, rather than laying down uniform rules, oblige the Contracting States to take the necessary measures in their domestic law to give effect to the provisions of the convention and secure their effective application.

In the EU realm, the GDPR operates a wide uniformization, but refers main issues to the law of the Member States, requiring developed domestic legislation to complement it. This legislation must provide appropriate solutions of substantive law, of Private International Law, and of International Public Law for those issues[68].

Bibliography

Antunes Varela, J. de M.: *Das Obrigações em geral*, 10th ed., Coimbra, 2004.

Baptista Machado, J.: *Lições de Direito Internacional Privado*, 2nd ed., Coimbra, Almedina, 1982

Brkan, M.: "Data Protection and European Private International Law", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal*, vol. 2, nº 43, 2015.

Capelo de Sousa, R.: *O Direito Geral de Personalidade*, Coimbra, Editora, 1995.

Christakis, T.: "Data, Extraterritoriality and International Solutions to Transatlantic Problems of Access to Digital Evidence. Legal Opinion on the Microsoft Ireland Case (Supreme Court of the United States)", *LSN Cyberspace Law eJournal*, vol. 23, nº 2, 2018.

Cooper, D. y Kuner, C.: "Data Protection Law and International Dispute Resolution", *Recueil des Cours*, t. 382, 2015, pp. 9–174.

Corneloup, S.: "De la loi applicable aux activités des entreprises de commerce électronique", *Rev. crit. dr. int. pr.*, 2017, pp. 112–122.

D Miguel Asensio, P.A.: "Competencia y Derecho aplicable en el reglamento general sobre protección de datos de la Unión Europea", *Revista Española de Derecho Internacional*, 2017, pp. 75–108.

De Miguel Asensio, P.A.: *Derecho Privado de Internet*, 5ª ed., Cizur Menor (Navarra), Civitas and Thomson Reuters, 2015.

De Sousa Gonçalves, A.: *Da Responsabilidade Extracontratual em Direito Internacional Privado. A Mudança de Paradigma*, Coimbra, Almedina, 2013.

Dias Oliveira, E.: "Algumas considerações sobre a responsabilidade civil extracontratual por violação de direitos de personalidade em Direito Internacional Privado", *Cuadernos de Derecho Transnacional*, nº 5, 2013, pp. 139–162.

Dias Oliveira, E.: *Da Responsabilidade Civil Extracontratual por Violação de Direitos de Personalidade em Direito Internacional Privado*, Coimbra, Almedina, 2011.

Dias Oliveira, E.:"A relevância do *right of publicity* no âmbito da propriedade intelectual", *Estudos de Direito Intelectual em Homenagem ao Prof. Doutor José de Oliveira Ascensão*, Coimbra, Almedina, 2015, pp. 228 ss.

[68] By International Public Law I mean rules dealing namely with the spatial scope of application of public law rules.

Dicey, Morris and Collins on the Conflict of Laws – 15th ed. by Lord Collins of Mapesbury (general editor), A. Briggs, A. Dickinson, J. Harris, J. McClean, P. McEleavy, C. McLachlan e C. Morse, London, Sweet & Maxwell and Thompson Reuters, 2012.

Erdos, D.: "European Union Data Protection Law and Media Expression: Fundamentally Off Balance", *Int. Comp. L. Q.*, vol. 65, 2016, pp. 139–184.

Fawcett, J. and Torremans, P.: *Intellectual Property and Private International Law*, 2nd ed., Oxford, Oxford University Press, 2011.

Ferrer Correia, A.: *Direito Internacional Privado. Alguns problemas*, Coimbra, Almedina, 1981

Fomperosa Rivero, A.: "Right to Be Forgotten in the European Court of Justice Google Spain Case: The Right Balance of Privacy Rights, Procedure, and Extraterritoriality", *LSN Cyberspace Law eJournal,* vol. 22, nº 19, 2017.

Keller, D.: "The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation", *LSN Cyberspace Law eJournal*, vol. 22, nº 19, 2017.

Kohler, Ch.: "Conflict of Law Issues in the 2016 Data Protection Regulation of the European Union", *Riv. dir. int. pr. proc.*, 2016, pp. 653–675.

Kropholler, J.: *Internationales Privatrecht*, 6th ed., Tübingen, Mohr Siebeck, 2006.

Kulk, S. and Borgesius, F.: "Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal,* vol. 4, nº 13, 2017.

Kuner, C.: "The Internet and the Global Reach of EU Law", *LSN Cyberspace Law eJournal*, vol. 22, nº 15, 2017.

Lima Pinheiro, L. de: "Direito aplicável à responsabilidade extracontratual na *Internet*", *Revista Faculdade de Direito da Universidade de Lisboa*, 42, 2001, pp. 825–834.

Lima Pinheiro, L. de: "O Direito de Conflitos e as liberdades comunitárias de estabelecimento e de prestação de serviços", *Seminário sobre a Comunitarização do Direito Internacional Privado*, 79–109, Coimbra, Almedina, 2005, pp. 79-109 (=*in Estudos de Direito Internacional Privado*, pp. 357–387, Coimbra, Almedina, 2006) pp. 102 ss.

Lima Pinheiro, L. de: "Reflexões sobre a governação e a regulação da internet, com especial consideração da ICANN", *Estudos de Direito Intelectual em Homenagem ao Prof. Doutor José de Oliveira Ascensão*, Coimbra, Almedina, 2015, pp. 363–385.

Lima Pinheiro, L. de: *Direito Internacional Privado*, vol. I, *Introdução e Direito de Conflitos. Parte Geral*, 3rd ed., Coimbra, Almedina, 2014.

Lima Pinheiro, L. de:*Direito Internacional Privado*, vol. II, *Direito de Conflitos. Parte Especial*, 4th ed., Coimbra, Almedina, 2015.

Mankowski, P.: "Das Internet im Internationalen Vertrags– und Deliktsrecht", *RabelsZ*,. 63, 1999, pp. 203–294.

Marques dos Santos, A.: *Direito Internacional Privado. Sumários*, 2nd ed., Lisbon, AAFDL, 1987

Miranda, J.: *Direitos Fundamentais*, 2nd ed., Coimbra, Almedina, 2017.

Moura Ramos, R.M.: *Da Lei Aplicável ao Contrato de Trabalho Internacional*, Coimbra, Almedina, 1991.

Moura Vicente, D.: *Da Responsabilidade Pré–Contratual em Direito Internacional Privado*, Coimbra, Almedina, 2001.

Nadeem, D.: "Territorial Limits to the European Union's Right to be Forgotten: How the CNIL Ignores Jurisdictional Basics in Its March 10, 2016 Decision Against Google", *Creighton Int'l & Comp. L.J.*. 8 2017, pp. 182–199.

Nunziato, D.: "The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten", *LSN Cyberspace Law eJournal*, vol. 23, nº 49, 2018.

Pissarra, N.A.: *O Dano Transnacional em Direito Internacional Privado. Alguns Problemas* (polycopied master dissertation), Lisbon, 2004, 153 ss.

Schwartz, P. and Peifer, K.–N.: "Transatlantic Data Privacy", *LSN Cyberspace Law eJournal*, vol. 22, nº 85, 2017.

van Calster, G.: "Regulating the Internet. Prescriptive and Jurisdictional Boundaries to the EU's 'Right to Be Forgotten', *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal,* vol. 2, nº 64, 2015 (available in SSRN).

Watts, S. y Richard, T.: "Baseline Territorial Sovereignty and Cyberspass", *LSN Public International Law: Foreign Relations & Policy Law eJournal*, vol. 5, nº 18, 2018 and *LSN Cyberspace Law eJournal*, vol. 23, nº 33, 2018.

Weber, R. (in collaboration with Grosz, M.): *Shaping Internet Governance: Regulatory Challenges*, Zurich, Basel and Geneva, Springer, 2009.

Woods, K.: "Against Data Exceptionalism", *LSN Transnational Litigation/Arbitration, Private International Law, & Conflict of Laws eJournal*, vol. 3, nº 16, 2016.