the SPANISH YEARBOOK of INTERNATIONAL LAW

The extraterritorial application of the EU Directive on data protection

Anabela Susana DE SOUSA GONÇALVES*

Abstract: At present, the processing of cross-border data flows has increased substantially. In the European Union, the 95/46/EC Directive established a harmonized system aiming to protect personal data. The need for legal security determines the importance of establishing in which situations the standard of protection of Directive 95/46/EC is applicable. This paper seeks to identify these situations, highlighting the extraterritorial application of the Directive and taking into account the current data processing techniques. The changes introduced by the proposed European Union Data Protection Regulation will also be analysed.

Keywords: 95/46/EC Directive – data protection – applicable law

DATA PROTECTION

Cross-border data flows have become regular with the technological evolution and with that the significance for individuals and economic agents of identifying which law governs data processing. In particular, it ought to be borne in mind that the internet is diffuse and global by nature for which reason the wide spreading of information across borders and the establishing of contacts and data exchange have become simple and consistent. The increase of cross-border flows of personal data has drawn attention towards the need to protect the privacy of the data subjects as a fundamental right,[1] on one hand, and to the importance of free flow of personal data for economic reasons, on the other hand, meaning that the use of information technology and the cross border flow of data have a "(...) unique function as a key element of infrastructure for efficient industries and a critical productivity enhancer [which] is crucial for sustaining recovery and laying the foundations for economies that are competitive in the long term".[2]

* Professor of Private International Law Law, Law School, University of Minho, asgoncalves@direito.uminho.pt.

[1] The right to privacy is recognized as a human right in: Article 12 of the Universal Declaration of Human Rights (adopted 10 December 1948), text available at http://www.un.org/en/universal-declaration-human-rights/, accessed 7 December 2015; in Article 17 of the International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976), text available at <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, accessed 7 December 2015; in Article 8 of the European Convention on Human Rights and Fundamental Freedoms (adopted 4 November 1950, entered into force on 3 September 1953), text available at <http://www.echr.coe.int/Documents/Convention_ENG.pdf>, accessed 7 December 2015; and in Article 11 of the American Convention on Human Rights (adopted 22 November 1969, entered into force on 18 July 1978), text available at http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm, accessed 7 December 2015. At a European level, the Charter of Fundamental Rights of the European Union distinguishes between the right of respect for private and family life (Article 7) and the right to protection of personal data (Article 8). The infringement of data privacy legislation has already been addressed by the European Court of Human Rights in several cases, as reported by G. Nardell, 'Levelling up: Data Privacy and the European Court of Human Rights', in S. Gutwirth, Y. Poullet and P. De Hert (eds), *Data Protection in a Profiled World* (Springer, Dordrecht, Heidelberg, London, New York, 2010) 43, at 43-52.

[2] As was recognized by the World Economic Forum in the *Global Information Technology Report 2009-2010, ICT for Sustainability*, at 7, available at < http://www3.weforum.org/docs/WEF_GITR_Report_2010.pdf>, accessed 10 June 2015.

 DOI: 10.17103/sybil.19.12

In the European Union (EU), the Directive 95/46/EC on the protection of individuals with regard to the protection of personal data and on the free movement on such data (Data Protection Directive) has established a harmonized system of protection of personal data considering that the divergences between Member States' legislations are an obstacle to the free flow of data and the development of the internal market (Recital 9). According to Recital 10 of this Directive, the approximation of the Member States' legislations would guarantee a minimal level of data protection in the EU and the free movement of personal information would become simpler. In pursuance of these goals of free flow of data and effective data protection, this Directive harmonizes the processing of personal data in the EU on the grounds of the principles of transparency, legitimate purpose and proportionality.[3]

Despite this harmonization, the need for legal certainty informs the significance of establishing in which situations the Directive 95/46/EC's standard of protection is applicable, to the extent that controllers that process personal data across borders ought to know which legislation they should comply with.

In everyday life, the processing of personal data occurs in several ways. Sometimes, personal data is collected by e-mail and other techniques; other times the data subject voluntarily puts his personal data online, for example in social networks like Facebook or Google Plus, and due to the global nature of the internet, in most cases these situations are related to more than one country. If the subject tries to revoke his consent and to retrieve his personal data, under which law can he do so? Sometimes, personal information is collected without the knowledge and consent of the subject and that information can be sold to other users. Other times, personal information can be collected by tracking the behaviour of the subject online by the website operators and this information can easily circulate across borders. The question is under which law is to be determined whether the processing of personal data is lawful or not. The establishing of the applicable law is more complex when one has to deal with globalization and new technologies, because "[...] companies are increasingly operating in different jurisdictions providing services and assistance around the clock; the internet makes it much easier to provide services from a distance and to collect and share personal data in a virtual environment; cloud computing makes it difficult to determine the location of personal data and of the equipment being used at any given time".[4]

[3] About the Data Protection Directive regime, see C. S. Castro, *Direito da Informática, Privacidade e Dados Pessoais* (Almedina, Coimbra, 2005), at 65-275.

[4] Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, Working Paper 179, 2010, at 6. The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC. According to Article 29, Section 2, the Working Party is composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission. The functions of the Article 29 Data Protection Working Party are stated in Article 30, Section 1: "1. The Working Party shall: (a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures; (b) give the Commission an opinion on the level of protection in the Community and in third countries; (c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms; (d) give an opinion on codes of conduct drawn up at Community level".

 DOI: 10.17103/sybil.19.12

The protection of personal data and the right to privacy in respect to the processing of personal data is different from country to country.[5] Even in the EU, despite the existence of the harmonization provided by the Data Protection Directive, there are different levels of protection of personal data to the extent that the Directive does not comprehensively regulate the protection of personal data and some matters are left to the national laws of the Member States. An example of the impact of the differences between domestic legislations in the cross-border flow of personal information is given by the European Commission: "[a] multinational company with several establishments in the EU has deployed an online mapping system across Europe which collects images of all private and public buildings and also takes pictures of people on the street. In one Member State, the inclusion of un-blurred pictures of persons unaware that they were being photographed was considered to be unlawful", but not in others.[6] This example shows the importance of determining the applicable law to the extent that the controller needs to know which substantive obligations he has to comply with when processing data; in other words, which data protection law he should obey.

Conflict rules[7] inform individuals and economic agents in which transnational situations are applicable the protection standards of the EU law that are consequently reflected in national laws of the Member States as a result of the transposition of the 95/46/EC Directive. The conflict rule that lays down the scope of application of Directive 95/46/EC is set in Article 4, and by analysing this provision, it can be concluded that the scope of application of the EU data protection legislation has been widened to the extent that it is possible to identify examples of its extraterritorial application that can raise problems of enforcement of the rights protected by Directive 95/46/EC. This paper seeks to identify these situations taking into account the current data processing techniques, and to examine the changes introduced by the EU Data Protection Regulation Proposal as well as the amendments made by the European Parliament to the latter.

---

5 As can be concluded by analysing the doctrine: see, *e.g.*, L. A. Bygrave, 'Privacy in a Global Context – A Comparative Overview', 47 *Scandinavian Studies in Law* (2004) 319, at 320-348; L. Kong, 'Data Protection and Transborder Data Flow in the European Context', 21 (2) *European Journal of International Law* (2010) 441, at 441-456; C. Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future', 187 *OECD Digital Economy Papers* (2011) 1, at 1-39; D. J. B. Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing, Copenhagen, 2013) at 39-45, explaining the different attitudes regarding privacy in common law countries and civil law countries, and between Europe, United States and Asia.

6 European Commission, *Safeguarding Privacy in a Connected World. A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM 9 final, Brussels, 2012, at 7.

7 In private relations related with more than one legal system, conflict rules determine which law shall apply and in which legal system the solution must be reached. About the choice of law problem, see B. Audit, *Droit International Privé* (4th ed, Economica, Paris, 2006) at 81-83; H. Batiffol and P. Lagarde, *Traité de Droit International Privé*, (8th ed, L.G.D.J, Paris, 1993) at 13-14; J. Fawcett and J. Carruthers, *Cheshire, North & Fawcett Private International Law* (14th ed, Oxford University Press, Oxford, 2008) at 8-9; B. Hoffman and K. Thorn, *Internationales Privatrecht einschließlich der Grundzüge des Internationalen Zivilverfahrensrechts* (Verlag C.H. Beck, München, 2005), at 177-178; G. Kegel and K. Schurig, *Internationales Privatrecht* (9th ed, Verlag C.H. Beck, München, 2004) at 300-325; Y. Loussouarn, P. Bourel and P. de Vareilles-Sommières, *Droit International Privé* (9th ed, Dalloz, Paris, 2007) at 62-78; P. Mayer and V. Heuzé, *Droit International Privé* (9th ed, Montchrestien, Paris, 2007) at 109-120.

 DOI: 10.17103/sybil.19.12

THE MATERIAL SCOPE OF APPLICATION OF THE DATA PROTECTION DIRECTIVE

The Data Protection Directive is applicable to the personal data processing in order to guarantee the right to privacy (Article 1). Thus, both, the wholly or partly by automatic means processing of personal data and the processing of personal data other than by automatic means which form part of a filing system or are intended to form part of a filing system, are submitted to the Directive (Article 3, Section 1).

Article 2 (a) of Directive 95/46/EC defines personal data as information relating to an identified or identifiable individual, such as an identification number, physical, psychological, economic, cultural or social factors related to him. Examples of the personal data processing are listed in Article 2 (b), being defined as any operation performed upon personal data, by automatic means or not such as, for example, the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction, of data. For example, the *Lindqvist* case provides us with a case of personal data processing, in which the European Court of Justice (ECJ) concludes that the operation of loading personal data on an internet page is to be considered processing of personal data for the purposes of Article 2 (b).[8] Similarly, it is considered data processing when "(...) the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results", even when the search engine does the same with other types of information and does not distinguish between these and the personal data.[9] These are some examples of personal data processing within the meaning of Article 4, Section 1 (a) of the Directive.

THE SPATIAL SCOPE OF APPLICATION OF THE DATA PROTECTION DIRECTIVE

The conflict rule that lays down the spatial scope of application of the EU standard of protection concerning personal data processing is set out in Article 4 of Directive 95/46/EC which also determines the applicable law. The underlying objective of Article 4 is the protection of individuals residing in the EU, by submitting the processing of their personal data to the safeguards laid down in the Directive. In that regard, the processing of data carried out by a person who is established in a Member State is governed by the law of that State. In addition, the data processing by a person established in a third state does not prevent the application of the standard of protection provided for in the Directive, as indicated later on. In other words, in these situations EU law may be extraterritorially applied. To this end, Article 4 provides for a broad scope of application of the Directive, whose purpose "(...) is primarily to ensure that individuals are not deprived of the

[8] *Criminal proceedings against Bodil Lindqvist*, Case C-101/01, 6 November 2003, ECR 2003 I-12971, §25.

[9] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, 13 May 2014, ECR 2014:317, §28; in the same direction, see *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, Case C-73/07, 16 December 2008, ECR 2008 I-09831, § 49.

 DOI: 10.17103/sybil.19.12

protection to which they are entitled under the Directive, and, at the same time, to prevent circumvention of the law".[10]

(1) Article 4, Section 1 (a)

According to Article 4, Section 1 (a), of the Data Protection Directive, the latter is applicable when the processing of personal data is carried out in the context of the activities undertaken by an establishment of the controller situated in the EU, and the law applicable is that of the Member State where that establishment is located. Accordingly, particular attention is to be paid to the location of the establishment and the nature of its activities.

The controller is the legal or natural person or entity that, alone or with others, decides which is the objective of the processing of personal data and the means used for that purpose, according to Article 2 (d) of the Data Protection Directive. Recital 47 helps to makes this concept clear by resorting to the example of the messages that contain personal data as the sole objective of transmission and are transmitted by e-mail or other communications technology; in this case "(...) the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates (...)" rather than the transmission service providers; however, the latter "(...) will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service".[11]

In the case of an online exchange of data, it may be difficult to determine the location of the relevant establishment to the extent that the activity of the controller on the internet may be scattered throughout several countries. The concept of "establishment" laid down in the Data Protection Directive helps to overcome this problem, given that it is broadly defined in Recital 19, namely, establishment is a stable arrangement through which an effective and real activity is exercised regardless of the form it takes such as a branch or a subsidiary. Therefore, only a stable establishment in a Member State is necessary to apply the law of that Member State, even if the main establishment is located in a third country. In those situations the data protection law of a Member State is applicable even if that activity has an extra-European dimension. Accordingly, the EU Directive applies extraterritorially. In the Google Spain Case, Google Inc., the parent company of the Google Group which had its seat in the United States, exploited the search engine Google Search and had a subsidiary - Google Spain (which had a separate legal personality and its seat in Spain) - for promoting the sale of advertising space generated on the website 'www.google.com'. Since the activity of Google Spain was to promote, facilitate and achieve the sale of online advertising products and services to third parties as well as the marketing of that advertising, essentially targeting businesses based in Spain through a stable arrangement in Spain, the ECJ considered that Google Spain was an establishment within the meaning of Article 4, Section 1 (a).[12] Google Spain was thus considered a stable arrangement through which an effective and real activity is exercised and therefore an

[10] Article 29 Data Protection Working Party, *Opinion 8/2010...*, *supra* n. 4, at 9.

[11] Under Article 2 (e), the controller must be distinguished from the processor, as the person or entity "(...) which processes personal data on behalf of the controller".

[12] *Google Spain SL*, *supra* n. 9, §49.

establishment as defined by Recital 19. Noteworthy is that a server or a computer will not usually be seen as an establishment, but only as a simple technical facility or instrument for the processing of information.[13]

If a controller has several establishments in different Member States, each one of them has to comply with the national rules of the Member States where they are located (Article 4, Section 1 (a) 2nd part). This rule chooses thus a mosaic approach that may lead to the situation in which the processing of personal data is subject to more than one national law:[14] for each personal data processing done by each establishment in the context of its activities, the law of the Member State of the location of each establishment, even if the controller is the same and the activity of personal data processing too. While national legislation is apparently based on the Directive on Data Protection and thus basically identical to that of other Member States, the divergence between data protection laws of Member States remains as a result of different transpositions of the Directive which is not completed either, meaning that it has loopholes. Accordingly, different laws could be applicable to the same situation, and that can lead to different results, thereby the coherence in regulating identical situations is impaired and the legal certainty undermined.

According to Article 4, Section 1 (a), the application of the law of a Member State is triggered provided that the location of the establishment is in that country, and that establishment actually processes personal data in the context of its activities. According to the ECJ, this concept should have a broad interpretation in accordance with Recitals 18 to 20 of the Directive and with the objective of protecting data subjects as established in the Directive.[15]

For the application of this Article, the location of users or data is not relevant. For example, in the case of a controller with an establishment in Austria that in the context of its activity processes personal data through its website accessible to users in several countries, the data protection governing law is the Austrian one.[16] A more complicated example is that of a controller established in Austria that outsources the processing to a processor in Germany.[17] As the processing in Germany occurs in the context of the activities of the controller in Austria, meaning that "(...) the processing is carried out for the business purposes of, and under the instructions given by the Austrian establishment, it is the Austrian law that is applicable to the processing carried out by the processor in Germany."[18]

One of the leading cases of application of Article 4 Section 1 (a) is the abovementioned Google Spain Case. In this case, the processing of the personal data by the search engine Google Search was

[13] Article 29 Data Protection Working Party, *Opinion 8/2010...*, *supra* n. 4, at 12.

[14] As is pointed out by L. A. Bygrave, 'European Data Protection, Determining Applicable Law Pursuant to European Data Protection Legislation', 16(4) *Computer Law & Security Report* (2000) 252, at 255.

[15] *Google Spain SL*, *supra* n. 9, §53-54.

[16] Article 29 Data Protection Working Party, *Opinion 8/2010...*, *supra* n. 4, at 13.

[17] *Ibid.*

[18] *Ibid.* However, according to Article 17, Section 3, the processor is also subjected to the law of the Member State in which he is established (Germany) in what concerns the implementation of appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

operated by a company seated in a third State (United States) which had an establishment in Spain, and it was considered that the processing of personal data was carried out in the context of the activities of that establishment "(...)if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable", to the extent that it was considered that the activities between the search engine and the establishment located in Spain were inextricably linked, meaning that the latter allowed to make profitable the search engine and this one needed the search engine to carry out its activities.[19] As the exhibition of personal data was accompanied by the display of an advertising linked to the search terms, the ECJ considered that the processing of personal data was carried out in the context of the activities of the controller's establishment in Spanish territory, on the grounds that the scope of Article 4, Section 1 (a) includes those situations where "(...) the operator of a search engine sets up a branch or subsidiary in a Member State which is intended to promote and sell advertising space offered by that engine and which positions its activity towards the inhabitants of that Member State".[20] The inextricable link between the personal data processing activities carried out by the search engine operated by a company located in a third country, and the activities of the establishment located in a Member State that directs its activities to that Member State, was the key element to consider that the personal data processing was carried out in the context of the activities of the establishment located in Spain. In other words, the Google Spain case teaches that the two key elements to the concept of personal data processing by the establishment in the context of its activities are: the inextricable link between the activities identified in the case and the direction of the establishment activities to a Member State.[21]

(2) Article 4, Section 1 (b)

The protection standard of the Data Protection Directive is also applicable when the place of the controller's establishment is situated in a third State in those cases where the national law of a Member State is applicable as a result of public international law [Article 4, Section 1 (b)] - the protection data law of that Member State will be applicable.

Under this rule fall the cases in which the controller does not have an establishment located in a Member State, therefore, the application of Article 4, Section 1 (a) is not possible. But the provision has a very limited scope, covering cases where the law of a Member State is applicable in a third State where the controller is established, due to public international law. That could be the case of an embassy, or a consulate, or a ship or a plane of that Member State. In these situations, the EU data

[19] *Google Spain SL*, *supra* n. 9, §55-56.

[20] *Ibid.*, § 57.

[21] It should be noted that the criterion of the direction of activities towards a certain State as a criterion of application has already been laid down in Article 6 of the Regulation No 593/2008, of 17 June 2008, on the law applicable to contractual obligations (Rome I) and Article 17, Section 1 (c) of the Regulation No 1215/2012, of 12 December 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I Recast), and has been applied by the ECJ in e-commerce international consumer contracts. For further developments, see A.S.S. Gonçalves, 'The E-Commerce International Consumer Contract in the European Union', 9 (1) *Masaryk University Journal of Law and Technology* (2015) 5, at 5-20.

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.

(3) Article 4, Section 1 (c)

The protection standard of the Data Protection Directive is also applicable when the controller is not established in the EU territory but uses equipment, automated or otherwise, situated in the territory of a Member State to process personal data. In such cases, the applicable law is that of the Member State where that equipment is located [Article 4, Section 1 (c)]. This provision has clearly an extraterritorial scope.

Section 1 (c) is only applicable where section 1 (a) of Article 4 is not. Accordingly, the former will only apply if the controller does not have an establishment located in the EU that is relevant for the activities in question; otherwise, Article 4 section 1 (a), is applicable. Article 4, section 1 (c), is also applicable if the controller has an establishment that is irrelevant to the application of Article 4, section 1 (a), to the extent that its activities are not related to the processing of personal data or to the processing of that specific personal data.[22] The justification of Article 4, section 1 (c), is to be found in Recital 20 of the Data Protection Directive that reads as follows: "whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice". This explanation enlarges the scope of application of the Directive and that of domestic Member States' legislation on data protection, meaning that EU provisions are applicable in situations where the processing of data is not undertaken in the European territory or in cases where the controller is established outside the EU. For example, in the case of individuals that upload personal data "onto an online social network operated from a server outside the EU",[23] the application of Directive 95/46/EC is possible in accordance with the terms of Article 4, section 1 (c), to the extent that, even if the controller's establishment is situated in a third State, the processing of the personal data is done through equipment situated in a Member State. Through this rule the application of the protective personal data rules of the EU is enlarged.

In order to apply this rule, the relevant factor is the use of equipment whose meaning needs to be determined. The concept of 'use of equipment' implies two factors: "(...) some kind of activity of the controller and the clear intention of the controller to process personal data", which does not require ownership or full control over the equipment for the processing from the controller,[24] i.e. one objective element, namely the activity of processing data by the controller; and one subjective element which is the intention to process personal data.

---

[22] Article 29 Data Protection Working Party, *Opinion 8/2010...*, *supra* n. 4, at 19.

[23] Kuner, *supra* n. 5, at 25.

[24] *Ibid.*, at 20.

 DOI: 10.17103/sybil.19.12

As to the concept of equipment is to be interpreted as an automated means to process data or otherwise, and this leads to a broad interpretation of such a concept as including "(...) human and/or technical intermediaries, such as in surveys or inquires", according to Article 29 Data Protection Working Party.[25] The application of a Member State law will be excluded if the equipment is used only for purposes of transit through the EU territory, like telecommunication networks (cables) or postal services that ensure communication transit to third countries. According to Article 29 Data Protection Working Party, this exception to the equipment criterion should be narrowly interpreted. However, it will have a limited application, because, as the Group points out, presently telecommunication services generally attach transit and added value services such as "spam filtering services and other manipulation of data at the occasion of their transmission", as the Group points out.[26]

The broad interpretation of equipment expands the application of Article 4, section 1 (c), and the extraterritorial application of the European data protection standards. This can lead to the application of the EU law to activities that have a weak connection with the EU. For example, the broad interpretation indicated entails the application of the EU law to activities done by processors located in the territory of a Member State on behalf of a controller established in a third State; in these cases, those controllers will have to comply with the law of that Member State.[27] In a similar vein, "(...) personal data collection through the computers of users, as for example in the case of cookies or JavaScript banners, trigger the application of Article 4 (1) c and thus of European data protection law to service providers established in third countries".[28] Finally, according to this broad interpretation, a controller established in a third State and using equipment in a Member State, although processing data of non-EU residents, triggers the application of Article 4, section 1 (c); thereby, this controller must comply with EU data protection legislation. In fact, all these situations involve the extraterritorial application of the EU data protection legislation and the question to be posed, in particular as regards to the last case, is whether there is a sufficient connection between those activities and the EU.

These situations of extraterritorial application of EU legislation raise problems of enforcement of the rights protected by Directive 95/46/EC. In this respect, Article 4, Section 2, determines that for the circumstances of section 1 (c) the controller must designate a representative established in the territory of that Member State, regardless of the legal actions which can be initiated against the controller himself. However, if the controller is located in a third State, it is not clear how legal actions can be initiated against him. Would a Member State court have jurisdiction? On which grounds? Should it have jurisdiction, would its decision be enforceable in a third State? Should it not have jurisdiction, would a court of a third State apply EU law?

This enforcement problem could be attenuated if the representative could be held responsible and sanctioned on behalf of the controller, but that would depend on the nature of the relationship

[25] Article 29 Data Protection Working Party, *Opinion 8/2010...*, *supra* n. 4, at 20.
[26] *Ibid.*, at 23.
[27] *Ibid.*, at 20.
[28] *Ibid.*, at 21.

 DOI: 10.17103/sybil.19.12

between the representative and the controller. However, the Directive does not clarify this aspect. As a consequence, "in some Member States, the representative substitutes the controller, also with regard to enforcement and sanctions, while in others it has a simple mandate. Some national laws explicitly foresee fines applicable to the representatives, while in other Member States this possibility is not envisaged".[29] The differences in transposing the Directive lead to insecurity and lack of uniformity with regard to sanctions that may result from failure to comply with the law of a Member State as a consequence of the application of Article 4. As a matter of fact, in some situations where the equipment is located in a Member State, the non-compliance with the EU data protection legislation will affect the controller located in a third State, and, in other cases, will not.

Some commentators of the Data Protection Directive accuse the EU of legislating for the world.[30] In fact, looking at the extraterritorial scope of the Directive, this is a valid statement. More specifically, it has been said that "extraterritorial jurisdictional claims are reasonable because if States do not extend their data protection to the conduct of foreign parties, they are not providing effective protection for their citizens".[31] In my opinion, the EU legislation will not be enforceable in most situations of extraterritorial application of the Data Protection Directive, the latter being a positive outcome in those cases where there is an insufficient connection with a Member State. However, a right that exists but cannot be enforced has no real meaning and that implies the weakening of that right. Consequently, these situations ought to be reduced.

THE EUROPEAN UNION DATA PROTECTION REGULATION PROPOSAL

The evolution of technology has unveiled that harmonization in Europe is far below the required level. The complexity of personal data processing as a result of information and communication technology has showed that there are relevant differences between the legislation of the Member States and the level of harmonization is thus deficient.[32] To change this situation, the European Commission presented a proposal of regulation concerning data protection in 2012.[33]

The proposed EU Data Protection Regulation tries to eliminate the differences in the protection of data privacy in the EU. The aim is to avoid the legal fragmentation that currently exists in the EU in order to achieve legal certainty, eliminate distortions of competition and build trust between economic operators and individuals with a view to helping the development of digital economy. It is

[29] *Ibid.*, at 23.

[30] Bygrave, *supra* n. 5, at 334; L. A. Bygrave, 'Determining Applicable Law pursuant to European Data Protection Legislation', 16 *Computer Law & Security Report* (2000) 252, at 257; P. Ford, 'Implementing the EC Directive on Data Protection – an outside perspective', 9 *Privacy Law and Policy Reporter* (2003) 141, at 149.

[31] D. Svantesson, 'Extraterritoriality in the Context of Data Privacy Regulation', 7(1) *Masaryk Journal of Law and Technology* (2012) 87, at 95.

[32] This lack of harmonization is repeatedly stated by the doctrine, see, e.g., P. De Hert and V. Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', 28 *Computer Law & Security Review* (2002) 130, at 132-141; R. Wong, 'Data Protection: The Future of Privacy', 27 *Computer Law & Security Review* (2011) 53, at 54-55.

[33] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM 11 final, Brussels, 2012, at 1-118.

made clear that it is essential to adjust the existing legal framework to the development of new technologies in order to favour the globalization of information and the transfer of personal data at an international level (inside the EU and between the Member States and third countries).[34] The proposed EU Data Protection Regulation enhances the data subjects' rights, enlarges data controllers' obligations,[35] and tries to eliminate the differences in the protection of individuals inside the EU, so that the processing of personal data may be equivalent in all Member States.[36]

In those situations covered by the proposed Regulation, the fact that it is directly and immediately applicable could solved the issue of determining the national data protection law applicable and it could lead to the saving of 2,3 billion Euro a year in terms of administrative burden to companies.[37] However, it is interesting to research to which situations related to third States would apply the rules of the proposed Regulation.[38] The question is whether the proposed Regulation maintains the same extraterritorial scope of application that can be found in the Directive in vigour to the extent that, as the European Commission has pointed out that there had been an "increased outsourcing of processing, very often outside the EU, and [it] raises several problems in relation to the law applicable to the processing and allocation of associated responsibility".[39]

The proposed Regulation maintains in Article 3, Section 1, the application of the EU legislation, to the processing of personal data in the context of the activities of a controller's establishment situated in a Member State. The proposed Regulation also determines its application when the establishment of the processor is situated in the European Union. The notion of "establishment" continues to be defined in a broader sense, to encompass the effective and real exercise of activities in the framework of stable arrangements regardless of the legal form of those arrangements (Recital 19 of the Regulation proposal). Accordingly, Article 3, Section 1, largely corresponds to Article 4, Section 1 (a), of the Data Protection Directive.

In line with Article 4, Section 1 (b), of the said Directive, Article 3, Section 3, lays down the application of the proposed Regulation to controllers established outside the Union, in a country where the national law of a Member State is applied as a consequence of public international law, for example, "(...) in a Member State diplomatic mission or consular post" (Recital 22).

However, the proposed Data Protection Regulation modifies the extraterritorial scope of the Directive. According to Article 3, Section 2, its provisions apply to controllers established in third States that process personal data of subjects residing in the EU provided that the processing activities

---

[34] European Commission, *Safeguarding...*, *supra* n. 6, at 7.

[35] For a detailed analysis, see P. Hert and V. Papakonstantinou, *supra* n. 25, at 132-141.

[36] European Commission, *Safeguarding...*, *supra* n. 6, at 20.

[37] According to figures given by V. Reding, 'The European data protection framework for the twenty-first century', 2(3) *International Data Privacy Law* (2012) 119, at 121.

[38] Besides, choice-of-law problems remain in situations not ruled by the proposed Regulation. As observed by Peter Blume, with this proposal harmonization will be improved, but it will be far from being ideal since many of the fundamental data protection provisions are drafted as open legal standards and need to be filled out by the national supervisory authorities: P. Blume, 'The myths pertaining to the proposed General Data Protection Regulation', 4(4) *International Data Privacy Law* (2014) 269, at 271-272.

[39] European Commission, *A comprehensive approach on personal data protection in the European Union, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM 609 final, Brussels, 2010, at 4.

are related to the offering of goods or services to such data subjects in the EU or the monitoring of their behaviour. Accordingly, the provision sets an accumulation of connections that can lead to the application of the EU law.

Both, the concept of activities related to the offering of goods or services and that of activities related to the monitoring of EU residents behaviour need to be determined, but this can be seen as a way of widening the protection of EU residents in a globalized world. Recital 21 of the Regulation Proposal helps to understand the meaning of the monitoring of the data subjects' behaviour by establishing that it includes "(...) data processing activities which consist of applying a 'profile' to an individual, particularly in order to make decisions concerning him or her or for analysing or predicting his or her personal preferences, behaviour and attitudes". For example, this covers all the techniques of data mining aimed to find out patterns of behaviour as well as the techniques of data warehouse as a way of storing personal data.

At first glance, the wording of this Article seems to reduce the application of European legislation to cases that have a weak link with the EU, like the example of a controller established in a third State, using equipment in a Member State, and processing data of non-EU residents. By not using the concept of *equipment located in a Member State*, this rule changes the application of the EU data protection standards in those cases where the controller is established in a third State: "[a] business established in the US that markets its products directly to EU residents, but has no physical presence in the EU, is not subject to the requirements of the Directive, but will be subject to the requirements of the Regulation".[40]

The accumulation of connecting factors when the controller is located in a third State appears to be a noble guarantee of the existence of a sufficient link between the activity and the EU. However, the proposed rule is not free from criticism. Since the proposed Regulation lays down that it only applies to the personal data processing of data subjects residing in the EU by a controller not established in the EU, that means that the Regulation will not be applied to data subjects temporarily travelling in a Member State provided that the processing is done by a controller not established in the EU, even if the data is collected in a Member State by the monitoring of their behaviour. This does not seem to be a reasonable outcome. Accordingly, it is necessary to ponder whether the provision laid down in Article 3, Section 2, of the proposed Regulation is satisfactory in the light of the concern of not applying EU data protection standards to situations that do not have a sufficient connection with a Member State.

The habitual residence of the data subject in the EU is one of the connections highlighted by the proposed Regulation as relevant in those cases where the controller is established in a third State, and it determines the application of the EU data protection legislation on grounds of establishing a link between the case and the EU in default of the connecting factor provided by the controller having an establishment in the EU. Nevertheless, this connecting factor excessively widens the extraterritorial

[40] Example taken from Hunton & Williams, The Proposed EU General Data Protection Regulation, A guide for in-house lawyers, 2015, at 10, text available at <https://www.hunton.com/files/Publication/e148d184-7b15-4e62-b295-0febc750f64d/Presentation/PublicationAttachment/a04eeb85-4b86-4034-a7ca-1ed5c3f50c56/Hunton_Williams_EU_Regulation_Guide_Overview.PDF>, accessed 15 June 2015.

application of EU data protection legislation to the extent that the latter would be applicable to EU residents even when the collecting and processing of data occurs when they are not in a Member State. "For example, an EU resident providing personal information during a holiday in New York would be protected by the EU data protection regulation by virtue of EU residence".[41] This is an example of a case with a weak connection with the EU, for which reason the application of EU law is not appropriate. This would be a case of extraterritorial application of EU law in which this law would hardly be enforceable. This example and the abovementioned one show that the habitual residence of the data subject is not an adequate connection to a Member State, according with the principle of proximity[42].

Pursuant to Article 3, Section 2, the controller must appoint a representative in each Member State of the residence of the subject whose personal data is processed in relation to the offering of goods or services to them or whose behaviour is monitored (Article 26, Section 1 and 3).[43] However, the nature of the relationship connecting the controller to his representative still remains to be defined in the proposal.

THE COMPROMISE TEXT OF THE REGULATION ADOPTED BY THE EUROPEAN PARLIAMENT

On 12 March 2014, the European Parliament adopted the report of the Committee on Civil Liberties, Justice and Home Affairs,[44] presented on 22 November 2013.[45] This text proposes some significant amendments to the Data Protection Regulation Proposal.

In relation to Article 3, section 1, of the proposed Regulation, the European Parliament adds that it ought to be applied to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, *whether the processing takes place in the Union or not*.[46] This can be useful if the processing takes place in a third State or in the cloud where one cannot specifically locate the processing of data.

Also in relation to Article 3, section 1, of the proposed Regulation, the European Parliament removes the residence of the data subject as a connecting factor when the controller has no establishment in the EU. Hence, the proposed Regulation ought to be applicable to the personal data processing of data subjects in the EU undertaken by a controller or *processor* not established in the EU provided that the processing is related to the offering of goods or services to such data subjects

41 Example taken from D. Svantesson, *Extraterritoriality...*, *supra* n. 5, at 107.

42 About the principle of proximity, see A.S.S. Gonçalves, *Da Responsabilidade Extracontratual em Direito Internacional Privado, A Mudança de Paradigma* (Almedina, Coimbra, 2013), at 158-165.

43 Without prejudice of the legal actions which can be initiated against the controller itself (Article 25, section 4).

44 Text available at <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402», accessed 15 June 2015.

45 Text available at <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0402&language=EN>, accessed 15 June 2015.

46 European Parliament, *I Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Jan Philipp Albrecht (rapporteur), COM (2012)0011 – C7-0025/2012 – 2012/0011(COD)), of 22.11.2013, adopted on 12 March 2014, at 63.

irrespective of whether a payment of the data subject is required;[47] or the monitoring of *such data subjects*.[48] As in the proposed Regulation, there seems to be a combination of connecting factors: the location of the processing of personal data, the nature of the activity and the activity directed to data subjects in the EU[49] The EU data protection standards would thus be applicable provided that the processing of personal data of the subjects occurs in the EU, and the processing activities are related to the offering of goods or services to them in the EU or the monitoring of such data subjects.

The adopted connecting factors solve the difficulties placed by the residence of the data subject. However, the rule raises questions and can be a source of uncertainty. For example, when should it be considered that the processing of personal data occurs in the EU? Which are the processing activities related to the offering of goods or services? Which are the processing activities related to the monitoring of data subjects' behaviour? Who is to be considered data subjects in the EU?

CONCLUSION

Having analysed article 4 of the Directive 95/46/EC, it can be concluded that the EU data protection standards are applicable in a number of cases with a weak connection to the EU, meaning that it is possible to identify examples of the extraterritorial application of this EU legislation that can raise problems of enforcement of the rights protected by the said Directive.

The extraterritorial application of the EU data protection legislation can result from the broad interpretation of "establishment" in Article 4, section 1 (a), or from the concept of use of equipment located in a Member State if the controller is not established in the EU [Article 4, section 1 (c)]. Both situations could lead to the non-application or lack of enforcement of the rights laid down by Directive 95/46/EC. Would a Member State court have jurisdiction in a situation where the controller is not established in the EU, but uses equipment located in the EU to process data of non-EU residents? On which grounds would it have jurisdiction? If it did have jurisdiction, would its decision be enforceable in a third State? If it did not have jurisdiction, would a court of a third State apply EU law?

The answer to these questions can be summarize concluding that EU data protection standards will not be enforceable in most situations of extraterritorial application of the Directive, and this is a reasonable outcome, at least in those situations where a sufficient connection with a Member State lacks. However, a right that exists but cannot be enforced has no real significance and it leads to the weakening of that right. The Data Protection Regulation Proposal aims to modify the connecting

[47] According to the amendment proposed by the European Parliament to the Recital 21, "in order to determine whether a processing activity can be considered to 'monitor' data subjects, it should be ascertained whether individuals are tracked, *regardless of the origins of the data, or if other data about them is collected, including from public registers and announcements in the Union that are accessible from outside of the Union, including with the intention to use, or potential of subsequent* use of data processing techniques which consist of applying a 'profile', particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes": *ibid*., at 8.

[48] European Parliament, *I Report on the proposal for a regulation...*, *supra* n. 46, at p. 63.

[49] The amendments proposed by the European Parliament to Article 25 erases the importance of the place of habitual residence of the data subject, stating that "the representative shall be established in one of those Member States where the offering of goods or services to the data subjects, or the monitoring of them, take place". *Ibid*., at 101.

factor for the application of EU law when the controller does not have a relevant establishment in a Member State. The proposed provision solves some situations, but it gives rise to further problems to the extent that other cases of extraterritorial application of EU legislation in situations with a weak connection with Member States. In contrast, the text adopted by the European Parliament and amending the proposed Regulation is slightly better.

The application of the EU data protection legislation to activities that have a weak connection to the EU should be avoided and cases of its extraterritorial application law should be reduced to the minimum necessary to implement its goals. The cumulating of connecting factors when the controller is located in a third State appears to be the best guarantee of the existence of a sufficient link between the activity and the EU, which is essential to safeguarding the legal certainty and ensuring the protection of legitimate expectations of the controller and the data subject.

The problem of enforcement would be attenuated if the representative of the controller that does not have a relevant establishment in the EU could be held responsible and sanctioned on behalf of the controller, which depends on the nature of the relationship between the representative and the controller. Regrettably, neither the Directive nor the Regulation proposal or the text approved by the European Parliament, clarify this element and it will continue to vary from Member State to Member State.

 DOI: 10.17103/sybil.19.12