UNIO - *EU Law Journal*. Vol. 4, No. 2, July 2018, pp 105-116.

School of Law – University of Minho

Finally: a coherent framework for the extraterritorial scope of EU data protection law ð the end of the linguistic conundrum of Article 3(2) of the GDPR

Graça Canto Moniz*

ABSTRACT: The extraterritorial scope of European Union's (EU) data protection law has been a controversial issue since the adoption of Directive 95/46/EC. The General Data Protection Regulation (GDPR) partially restructures the terms of the extraterritorial reach of EU data protection law and introduces new elements to an old debate. This contribution seeks to address one of those elements, concerning a linguistic ambivalence found in Article 3 (2) of the GDPR, and stress the practical consequences that emerge from this conundrum.

KEYWORDS: General Data Protection Regulation – extraterritoriality – Article 3 (2) – linguistic problems – coherent framework.

* PhD candidate at NOVA Direito. Co-cordinator of the "Observatório de Proteção de Dados Pessoais".

I. Introduction[1]

The debate surrounding the extraterritorial scope of EU data protection law is not new.[2] After a period of raising limited concern and passing largely unnoticed, the discussion was fueled, first, by the *Google Spain* ruling.[3] In this case, the Court of Justice of the European Union (CJEU) found that EU data protection law applies to the activities of Google Inc. established overseas. Secondly, the provisions on the territorial scope of EU data protection law have gained more attention with the adoption of the EU GDPR.[4]

There are several aspects of the current debate: first, the question surrounding the legitimacy of the extraterritorial scope of the GDPR and the demand for the EU to exercise jurisdictional restraint[5]; secondly, there are authors who welcome GDPR's new criteria as "*revolutionary game changers*" and emphasize the need to ensure effective protection[6]; and, lastly, there are those that stress the difficulties concerning the enforceability of the EU's jurisdictional claim.[7]

This article aims to introduce a new element to this discussion highlighting a problem identified in different official versions of the GDPR regarding its territorial scope. After a short description of the previous territorial scope (1) under Directive 95/46/EC[8], this paper will then (2) underline the new rules set on the GDPR[9]; look at the criteria established in Article 3(2) of the English version of the GDPR and compare them (3) with the rules outlined in the same Article in other official versions of the GDPR; I will then (4) demonstrate the practical consequences of the linguistic

[1] This article was written with the financial support of "Fundação para a Ciência e Tecnologia" ("FCT"). I must thank Francisco Pereira Coutinho and Gabriela Zanfir for the brief but important exchange of ideas regarding the subject of this article.

[2] Yves Poullet, "Transborder Data Flows and Extraterritoriality: the European Position", *Journal of International Commercial Law and Technology* 2 (2007): 141; Joshua Bauchner, "State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate", *BJIL* 26 (2000-2001): 696; Lee Bygrave, "Determining Applicable law pursuant to European Data Protection Legislation", *CLSR* 16 (2000): 252; Lokke Moerel, "Back to basics: when does EU data protection law apply?", *IDPL* 1(2) (2011): 97; and "The long arm reach of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", *IDPL* 1(1) (2011): 30; Article 29 Data Protection Working Party, "Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites", 30 may, 2002.

[3] Judgment *Google Spain SL and Google Inc.* v. *Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* Case C-131/12, May 2014, ECLI:EU:C:2014:317.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[5] Merlin Gomann, "*The new territorial scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement*", Common Market Law Review 54 (2017): 567; Brendan Van Alsenoy, "Reconciling the (extra) territorial reach of the GDPR with public international law", *Data Protection and Privacy under Pressure,* ed. Gert Vermeulen and Eva Lievens (Antwerp: Maklu Publishers, 2017), 77-98; Christopher Kuner, "Extraterritoriality and regulation of international data transfers in EU data protection law", *International Data Privacy Law* 5 (2015): 235.

[6] Ulrich Dammann, "Erfolge und Defizite der EU-Datenschutzgrundverordnung", *Zeitschrift für Datenschutz* (2016): 307.

[7] Christopher Kuner, *Extraterritoriality and regulation*…, 244.

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data.

[9] According to article 94 (1) GDPR, "Directive 95/46/EC is repealed with effect from 25 May 2018".

ambivalence identified before, in the literature and in the Portuguese legislative proposal implementing the GDPR; and (5) the Author will explore the solution finally advanced by the Council of the EU in May 2018.

II. The territorial scope of EU data protection law under Directive 95/46/EC

The applicability of EU data protection law was laid down in Article 4 of the Directive 95/46/EC, namely the scope of law both *within* and, for what is relevant for this paper, *outside* the EU. From the perspective of transnational companies, Article 4 was the most important provision in the Directive since it governed whether any of its rules applied to them in the first place. On the other side, it was also an important provision from the perspective of the data subject as it established the terms and limits of the protection afforded in EU data protection law. However, despite this relevance, several authors criticized this provision stating that it was "*poorly constructed*"[10] and underlined the "*difficulties in determining whether EU data protection law applies to processing of personal data in the new technical global environment*".[11]

In practice, Article 4 hinged on two main rules: one relating to data controllers *established* in the EU (1.1) and another for non-EU controllers (*not* established in the EU) (1.2.).

a. Data controllers established in the EU

According to Article 4(1)(a), the Directive 95/46/EC was applicable when "*the processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of the Member State (…)*". According to CJEU case-law, a two-step test was set out to determine the applicable law under this provision: first, there must have been an establishment of the data controller on the territory of a Member State and, secondly, it was necessary that the "*processing of personal data by the data controller be carried out in the context of the activities*" of that establishment.[12] So, one needed to clarify what was a data controller (1.1.1), when did it have an establishment (1.1.2) and, lastly, when was the processing carried out in the context of the activities of that establishment (1.1.3.)?

i. What is a data controller?

According to Article 2 (d) of Directive 95/46/EC, a data controller was the "*natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*".

ii. What is an establishment?

The concept of establishment was broadly defined in Recital 19: "*implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or subsidiary with a legal personality, is not the determining factor in this respect*". This means that neither the *nationality* of the data controller, the place of

[10] Liane Colonna, "Article 4 of the EU Data Protection Directive and the irrelevance of the EU-US Safe Harbour Program", *International Data Privacy Law* 4(3) (2014): 207.

[11] Douwe Korf, "New Challenges to Data protection", Working Paper No. 2: Data protection laws in the EU, *European Commission DG JFS,* January 2010.

[12] Judgment *Google Spain*, paragraph 50; and Judgment *Weltimmo s.r.o.* v. *Nemzeti Adatvédelmi és Információszabadság Hatósag,* Case C-230/14, October 2015, paragraph 28 *et seq*., ECLI:EU:C:2015:639.

its *main establishment* or the *physical location* of the processing were relevant for EU law to apply. Accordingly, EU data protection law might be applicable even if the main establishment was located abroad or in a third country. The paradigmatic *Google Spain* ruling illustrates this situation.

Despite being extensively debated with respect to the "*right to be forgotten*", *Google Spain* is a game changer when we look at the CJEU's interpretation of Article 4(1)(a) of Directive 95/46/EC.[13] In fact, this is the only case where the CJEU was required to rule on the applicability of EU data protection law to a data controller with the main establishment in a third country. Google Inc., the parent company of the Google Group, which had its seat in the United States and exploited the search engine Google Search, was considered the data controller[14] and its subsidiary, Google Spain, the establishment.[15]

In the *Weltimmo* case, the court advocated a "*flexible definition of the concept of 'establishment'*".[16] The CJEU found that a data controller is established in a Member State when he as a "*real and effective activity*", even if a *"minimal one"*, which can consist of running a real estate website, concerning properties in that Member State and written in the language of that Member State[17]; secondly, the presence of a representative serving as point of contact, alongside other elements such as a bank account or a post office box, were also highlighted by the CJEU.[18] In the *Amazon* case, the CJEU merely clarified that "*an establishment cannot exist merely because the undertaking's website is accessible" from a certain Member State*".[19]

iii. When is the processing carried out in the context of the activities of the establishment?

The second moment of the test applied by the CJEU concerns the condition that processing be carried out "*in the context of the activities*" of the establishment. As explained by Moerel, the most straightforward example of this is when a multinational company process data centrally outside the EU: "*a foreign parent company often also processes data of its EU group companies for central management purposes. If that processing also takes place in the context of the activities of these EU group companies (for instance, the foreign parent company operates a central HR system both for its own central management purposes, but also for HR purposes of the EU group companies), the EU data protection laws will apply to those parts of the central processing which relates to the respective employees of the EU subsidiaries*".[20]

Recently, the CJEU has, for at least two times, clarified the terms of this condition. The first, and more relevant, was the *Google Spain* ruling, where the court adopted a teleological interpretation of Article 4 (1) (a) of Directive 95/46/EC aiming to ensure "*an effective and complete protection of the fundamental right (…) to privacy*".[21] In light of this, the CJEU advocated new criteria to ascertain in which

[13] Merlin Gomann, *The new territorial scope*…, 569.
[14] Considering a search engine a "controller" triggered a lot of criticism, Christopher Kuner, "The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines", *LSE Law, Society and Economy Working Paper,* (2015): 9.
[15] Judgment *Google Spain*, paragraph 48.
[16] Judgment *Weltimmo*, paragraph 29.
[17] Judgment *Weltimmo*, paragraph 32.
[18] Judgment *Weltimmo*, paragraph 33.
[19] Judgment *Verein fur Konsumenteninformation* v. *Amazon EU Sàrl,* Case C-191/15, July 2016, paragraph 76, ECLI:EU:C:2016:612.
[20] Lukke Moerel, *The long arm reach of EU data protection law*…, 30.
[21] Judgment *Google Spain*, paragraphs 53 and 54.

situations the processing is "*carried out in the context of the activities of the establishment*": when there is an "inextricable link" between the activities of the EU establishment and the processing of the non-EU data controller.[22] In *Google Spain*, the Court stated that, despite the processing of personal data for the purposes of the service of a search engine (Google Search)[23] is carried out exclusively by Google Inc., the activities of Google Spain (promotion and selling of online advertising space) are "*inextricably linked*" to that processing since "*the activities relating to advertising space constitute the means of rendering the search engine at issue economically profitable*".[24] Without the advertising activities of Google Spain and similar subsidiaries across the globe, it would not be economically feasible for Google to offer its services. This means that the processing performed by Google Inc. is *economically* sustained by the activities of it Spanish establishment.

But the "inextricable" connection between the processing performed by Google Inc. and the activities of its establishment is not merely economic: it is also *online*.[25] When Google Inc. displays personal data on a search results page in Spain, that processing "*is accompanied, on the same page, by the display of advertising activity of the controller's establishment on the territory*" of Spain; hence, for the CJEU, it was "clear" that the processing of personal data by Google Inc. "*is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State*".[26]

The second decision was the *Weltimmo* case where it is stated that the CJEU significantly diminished the role of this second moment.[27]

b. Data controllers not established in the EU

i. Article 4(1)(b)

As stated in this provision, when the data controller is *not* established in an EU Member State, Directive 95/46 was applicable as result of public international law. This provision has a very limited scope: for example, when the data controller is an embassy, a ship or a plane located in a third state. It has been stated that "*in these situations, data protection legislation does not have a truly extraterritorial application, since the application of the law of a Member State in a third State results from public international law and occurs in circumscribed cases*".[28]

---

[22] Merlin Gomann, *The new territorial scope of EU Data Protection Law*…, 572.

[23] "In exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine '*collects*' such data which it subsequently '*retrieves*', '*records*' and '*organizes*' within the framework of its indexing programs, '*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. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data." – Judgment *Google Spain*, paragraph 28.

[24] Judgment *Google Spain*, paragraph 56.

[25] Merlin Gomann, *The new territorial scope of EU Data Protection Law*…, 574.

[26] Judgment *Google Spain*, paragraph 55.

[27] Merlin Gomann, *The new territorial scope of EU Data Protection Law*…, 573.

[28] Anabela de Sousa Gonçalves, "The extraterritorial application of the EU Directive on data protection", *Spanish Yearbook of International Law*, 19 (2015): 202.

ii. Article 4(1)(c)

Directive 95/46 was also applicable to the processing of personal data where 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 the purposes of transit through the territory of the Community*". The reason for this Article is found in Recital 20: "*whereas the fact 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 and used are located, and there should be guarantees to ensure the rights and obligations provided for in this Directive are respected in practice*".

The notion of "equipment" [Article 4 (1) (c)] or "means" (Recital 20), crucial to determine the applicability of this provision, was broadly interpreted to entail "*personal data collection through the computers of users, as for example in the case of cookies or JavaScript banners*", triggering "*the application of Article 4 (1) (c) to service providers established in third countries*".[29] Also, according to this broad interpretation, a data controller established in a third country that uses equipment in a Member State to process personal data of non-EU nationals or residents is bound by Directive 95/46. Since this interpretation significantly expands the extraterritorial scope of EU data protection law, some authors questioned whether, in these situations, there was a sufficient connection between the foreign activities and the EU and wondered about the EU's legitimacy to legislate "*for the world*".[30] The CJEU never had the chance to validate this broad understanding of Article 4 (1) (c) since the request for a preliminary ruling in the *Rease et Wullems* case was withdrawn.[31]

Article 4 (1) (c) gained more importance over the years with the development of new technologies and, in particular, of the Web version 2.0, which facilitates the collection and processing of personal data at a distance and irrespective of any physical presence of the data controller in the EU.[32] The problem, however, was the practical and "undesirable" consequences of applying this provision to data controllers located outside the EU in terms of enforceability and when there was no real connection with the EU.[33]

III. What is new in the GDPR?

In 2010, the European Commission ("EC") acknowledged the need to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that would allow the digital economy to develop across the Internal Market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities[34]. In fact, Directive 95/46 was

[29] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", 2010: 21.

[30] Anabela Gonçalves, *The extraterritorial application*…, 203; Dan Svantesson, "Extraterritoriality in the Context of Data Privacy Regulation", *Masaryk Journal of Law and Technology,* 7, 1 (2012): 95; Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", 29.

[31] Request for a preliminary ruling from the *Raad van State (the Netherlands)* lodged on 24 April 2015 – *TD Rease and P Wullems;* other party: *College bescherming persoonsgegevens.*

[32] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", 19.

[33] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", 24 and 29.

[34] European Commission, "A comprehensive approach on personal data protection in the European Union", November 2010.

affected by the "*challenge of regulatory connection*"[35], "*pacing problem*"[36], and "*Collingridge dilemma*"[37], in the sense that the normative solutions prescribed in 1995 were (obviously) not adequate in light of technological and business developments that have brought new challenges for the protection of personal data. Additionally, another drawback of Directive 95/46 concerned the relevant differences between the legislation of EU Member States, making the level of harmonization deficient.

Two years later, the EC presented a proposal for a regulation that later became the GDPR.[38] This new framework changed the rules on the territorial scope, especially for the case where data controllers are *not* established in the EU, echoing a proposal from the data protection authorities in 2010 pledging for a "*more specific connecting factor, taking the relevant 'targeting' of individuals into account*".[39] Then it was also stated that "*such a criterion is not new and has been used in other context[s] in the EU, and by the United States legislation (…)*".[40] Two main reasons explain this proposal: the "undesirable" consequences surrounding the application of Article 4 (1) (c) and the tendency that processing operations by companies outside the EU increasingly target data subjects for advertising and selling products and services online.

Let us see the exact terms of this new rule in Article 3 (2) of the GDPR (2.2.). However, before, we must highlight the (small) changes in Article 3 (1) for data controllers *and* processors established in the EU (2.1.). It is worth mentioning that the provision concerning the applicability of the GDPR according to international public law, Article 3 (3), remains the same as Article 4 (1) (b) of Directive 95/46.

a. Data controllers and processors established in the EU

Article 3(1) of the GDPR maintains the principle that data protection legislation applies if data is processed in the context of activities of an establishment of a data controller on Union territory, while adding, after data controller, "*or a data processor*". In practice, this means that processors are also directly bound by the GDPR and must comply with several impositions such as Article 30 (2) (records of processing activities), Article 31 (cooperation with the supervisory authority), Article 32 (security of processing), Article 33 (2) (notification of personal data breach), Article 37 (designation of the data protection officer) and Article 44 (transfers of personal data to third countries or international organizations).

The GDPR also adds that, when the data controller or processor is established in the EU and the processing is in the context of the activities of that establishment, it is not relevant if the "*processing itself takes place within the Union*". This aims to clarify that it is not necessary that the establishment *itself* takes part on the processing, as was the case in *Google Spain.*

---

[35] Roger Brownsword, *Rights, Regulation and the Technological Revolution* (Oxford: OUP, 2008).

[36] Braden Allenby, "Governance and technology systems: the challenge of emerging technologies", in *The growing gap between emerging technologies and legal-ethical oversight,* ed. Gary Marchant *et al.*, (Amsterdam: Springer, 2011).

[37] David Collingridge, *The social control technology* (s/d: Pinter, 1980).

[38] 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", COM/2012/011 final - 2012/0011 (COD).

[39] Article 29 Data Protection Working Party, "Opinion 8/2010 on applicable law", 24.

[40] *Ibidem.*

b. Data controllers and processors not established in the EU

According to the English official version, Article 3 (2) states that the GDPR "*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*".

Recitals 23 and 24 further explain what the aim of the EU legislator was. Recital 23 states that: "*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 this 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. Explaining what is meant by monitoring of the behavior of data subjects, Recital 24 highlights that "*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.*"

This new geographical scope of the GDPR is considered by some scholars as the most controversial aspect of the new regulation.[41] Nevertheless, in our view, the new scope of application of the GDPR is reduced when compared with Article 4 (1) (a) of Directive 95/46. It is arguable that the data controller established in a third country will always have a strong connection to the EU in the sense that he processes personal data of subjects located there and his activities are *directed* to the EU market, its consumers or, generally, "*the trading community of the EU*".[42] As stated by Alsenoy, "*the primary nexus with EU territory is not the presence of a controller or processor within the EU, but rather the location of the data subjects to which the relevant activities [the offering of goods or services and the monitoring of behavior] are targeted*".[43] De Hert and Czerniawski describe this as a "*destination approach*" and present a strong defense of Article 3 based on the idea that foreign operators will not be surprised by EU Law since they will only be targeted by EU law if they target the EU.[44]

---

[41] Dan Svantesson, "Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation", *International Data Privacy Law* 5 (2015): 230.

[42] Merlin Gomann, *The new territorial scope of EU Data Protection Law*…, 586.

[43] Brendan Van Alsenoy, *Reconciling the (extra) territorial reach*…, 94

[44] Paul de Hert and Michal Czerniawski, "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context", *International Data Privacy Law* 6 (2016): 231.

In fact, what is relevant is not the place of establishment of the data controller but the physical location of the data subject in the Union, whether domiciled, residing or temporarily traveling, whatever their nationality. This is in line with the aim of the former Directive[45] and the GDPR to ensure protection to *all natural persons*, whatever their nationality or place of residence, according to Recitals 2 and 14. Two examples illustrate this rule: (1) a national from a Member State provides personal data during a holiday in the USA to a data controller established in that country – he/she is not protected by the GDPR since he/she is not located in EU territory; (2) a Chinese tourist during his/her holiday in Portugal provides his/her personal data to a data controller established in a third country that, through its online website, sells its products in the EU – he/she is protected by the GDPR since he/she is located in EU territory when he/she buys the product.

Despite the many questions surrounding Article 3 pointed out in the literature[46], namely the difficulties in enforcing law to a foreign entity with no physical presence in the EU, this paper focusses on another issue.

IV. Different wording of Article 3(2) in official versions of the GDPR

The problem I would like to highlight is only detected when one compares the official English version of the GDPR[47] with, for example, the Portuguese and the Spanish versions. The main feature of these two official versions was that in Article 3 (2), the extraterritorial scope of the GDPR was different from the English one – and so it was until very recently, as we shall see at the end of this text. According to the wording of those two versions, the GDPR applied to the processing of personal data of data subjects *residing*[48] in the EU by a data controller or processor not established in the EU. This means that, in our example, the Chinese tourist could not benefit from the protection afforded by the GDPR since he/she is not a *resident* in the EU. However, if he/she was buying his/her product in the UK, even in France or Italy, the situation would be different.

In our view, this wording was in clear contradiction with the real intention of the EU legislator to protect *all* data subjects located in the Union despite they not being residents in any Member State.[49] First, we could state that Article 8 of the EU Charter of Fundamental Rights (CFREU) is clearly applicable to any individual and not only residents in the EU ("*Everyone* has the right to the protection of personal data concerning him or her"). Nevertheless, one could argue that the condition of residency of the data subject stated in Article 3 (2) of the Portuguese and Spanish versions consists of a legitimate restriction of the subjective scope of the fundamental right to data protection if conditions in Article 52 CFREU are met. This argument could hardly be successful since the CJEU has previously stated that EU legislation

[45] Recital 2.

[46] Anabela de Sousa Gonçalves, *The extraterritorial application*…, 208; Brendan Van Alsenoy, *Reconciling the (extra) territorial reach*…, 90; De Hert and Czerniawski, *Expanding the European data protection scope*…, 238; Dan Svantesson, *Extraterritoriality and targeting in EU data privacy law*…, 226; Merlin Gomann, *The new territorial scope of EU Data Protection Law*…, 584.

[47] As well as the Italian and French versions, among others.

[48] "*Residentes no território da União*" (Portuguese version), "*interesados que residan en la Unión*" (Spanish version).

[49] Pedro Asensio, "Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europeu", *Revista española de Derecho internacional* 69(1) (2017): 89.

restricting fundamental rights must lay down "*clear and precise rules*" governing the "*scope and application*" of the restriction.[50] A restriction of a fundamental right expressed only in some official versions of the same legal act can hardly be considered "*clear and precise*".

Second, the first proposal of the GDPR by the EC, stating the condition of residence of the data subject, was rejected by the European Parliament[51] and there is no evidence of a different position of the Council. As matter of fact, the Council mentioned, in March 2016, regarding the territorial scope of the GDPR that "*(…) the Regulation applies to the processing of personal data of data subjects who are in the Union, even if a controller or processor is not established in the Union, but where its processing activities are related to the offering of goods or services to such data subjects in the Union, as well as the monitoring of their behavior as far as their behavior takes place within the European Union*".[52] This is in accordance with its position regarding Article 3 (2) from April 2016.[53]

Third, following a systematic reading of the GDPR, in *all* official versions, the wording of Recitals 2 and 14 is the same, clearly stating the irrelevance of the place of residence of the data subject when applying the GDPR. Also, according to Article 3 (1) of the GDPR, for example, a citizen or resident in the USA might demand access to his data from a data controller with an establishment in the EU when the data is processed in the context of that establishment.[54]

V. The unintended consequences of a linguistic ambivalence

The problem we stress is not merely theoretical. One could say that the practical consequences of the linguistic ambivalence previously noted are irrelevant since they are only felt outside the EU. However, if the EU intends to exercise extraterritorial jurisdiction, and wants to be taken seriously, it should be more coherent. As stated by De Hert and Czerniawski, "*when deciding for or against extraterritorial jurisdiction a legislator has to assess many factors. The challenge for the EU legislator is to balance flexibility of the territorial scope, required in the digital age for the data protection law to be effective (for example, in order to avoid forum shopping), with legal certainty for entities and persons outside the EU processing personal data of individuals in the EU. The stakes for controllers and processors are high: a small American*

[50] Judgment *Maximilian Schrems* v. *Data Protection Commissioner,* Case C-362/14, 6 October 2015, paragraph 91, ECLI:EU:C:2015:650.

[51] European Parliament legislative resolution of 12 March 2014 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, amendment 97.

[52] "Draft Statement of the Council's Reasons", Council of the European Union, 17 March 2016, 7, accessed 10 May 2018, http://data.consilium.europa.eu/doc/document/ST-5419-2016-ADD-1/en/pdf.

[53] "Position of the Council at first Reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", 8 April 2016, 110.

[54] This was a question raised during the investigation concerning *Cambridge Analytica*. The ICO, where that data controller is established received a complaint from a US citizen regarding his personal data processed in the context of the activities of Cambridge Analytica's establishment in the UK: "(...) his data was being processed in the UK by Cambridge Analytica, and the Data Protection Act 1998, the GDPR that follows it and the Data Protection Bill do not make distinctions as to citizenship. It does not matter that he is a US citizen (…)". See "Oral Evidence: Fake News", House of Commons, Digital, Culture, Media and Sport Committee, last modified 6 March 6, 942, accessed 10 May 2018, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/fake-news/oral/79824.pdf.

entrepreneur doing business globally will suddenly be faced with the message that he or she will have to comply with EU law in addition to US law".[55] However, if such linguistic divergence had been maintained, a foreign operator not only would have had to comply with the law from his/her country of origin but also with different versions of EU law and, as we will see, different versions of national law implementing the GDPR. The result is the implementation of a confusing framework from the perspective of foreign operators that might have created loss of confidence in the (already questioned) legitimacy of EU's exercise of extraterritorial jurisdiction.

But the consequences of this linguistic ambivalence are also reflected in the literature about Article 3 of the GDPR and in the national legal acts implementing it. First, in the literature, if there are authors who don't event tackle this question[56], others state that the real criterion is the residency of the data subject in the EU[57] which is a viewpoint echoed by others.[58] Secondly, reflecting the consequences of this linguist variance, the Portuguese governmental proposal implementing the GDPR ("*Proposta de Lei 120/XII*") originally adopted the condition of residence as stated in the Portuguese official version of Article 3 (2) of the GDPR. In fact, Article 2 (2) (b) of that proposal states the "*present law is also applicable to the processing occurring outside of the national territory when (…) it affects data subjects residing in the national territory, when the processing activities are covered by number 2 of article 3 of the GDPR (…)*". Luckily, this wording of Article 2 (2) (b) of "*Proposta de Lei 120/XII*" was criticized by the Portuguese data protection authority[59] and is currently being discussed in the Portuguese Parliament.[60]

VI. Conclusion: solving the linguistic conundrum of Article 3 (2) of the GDPR

After two years and many academic articles written about Article 3 (2) of the GDPR, the linguistic problem was finally settled. On 19 April 2018, the Council of the European Union adopted a "*corrigendum/rectificatif*" concerning all linguistic versions.[61] In this document we can find, among other corrections, amendments to Article 3 (2) of the Portuguese and Spanish official versions abolishing the criteria of residency and adopting the same wording of the English version.[62]

From now on, there can be no doubt that, for the GDPR to be applicable, the place of residence of the data subject in the territory of the EU is irrelevant. Let us hope that the Portuguese legislator reads page 278 of this "*corrigendum*".

---

[55] De Hert and Czerniawski, *Expanding the European data protection scope beyond territory*…, 239.

[56] De Hert and Czerniawski, *Expanding the European data protection scope beyond territory*…, 237.

[57] Maja Brkan, "The unstoppable expansion of the EU Fundamental Right to Data Protection", *Maastricht Journal of European and Comparative Law*, 23, 5 (2016): 834, "(…) *a third-country controller processing personal data subjects residing in the Union will have to respect the European data protection standards prescribed by the GDPR* (…)".

[58] Pedro Asensio, *Competencia y Derecho aplicable en el Reglamento General sobre Protección de Datos*…, 89.

[59] "*Parecer 20/2018*", Comissão Nacional de Proteção de Dados Pessoais, Case 6275/2018: 5v.

[60] All information is available at http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368.

[61] Document number 8088/18, Council of the European Union, 19 April 2018, accessed 10 May 2018, http://data.consilium.europa.eu/doc/document/ST-8088-2018-INIT/en/pdf.

[62] For the Spanish version, page 13, and for the Portuguese version, page 278. The *corrigendum* was published in OJ L 127/2, 23.5.2018.