The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation

by **Adèle Azzi***

Abstract: The General Data Protection Regulation (GDPR) imposes a significant burden of compliance on overseas businesses which process personal data of EU individuals. An impressive number of articles warns about the new risks incurred by data processors around the world; be they one of the Internet giants, or a non-EU company which dared to offer goods to EU consumers, or that had the idea to use cookies on its website to track EU consumers. However, does the EU actually have the necessary means to ensure that the rules are followed by all? And if not, is the EU equipped to enforce compliance? Those are legitimate questions in the light of the context in which the EU has extended its jurisdiction. Not only has it been decided unilaterally, but such rules are to be enforced in cyberspace, in an international context, and on operators, which may not have any physical presence in the EU. One may think that processors have no reason to panic, there is little chance that the GDPR enforcers will find them and force them to comply under the threat of fines. Yet, internet users witness an undeniable wave of change in the terms of the use and processing of data on a majority of websites. Does this phenomenon reveal a real power of enforcement on the EU side? This work attempts to answer this question by analysing two factors which greatly impact the efficiency of extraterritorial claims. First, the legitimacy of the extraterritorial claim. Through the application of international law principles, it will be seen that the extraterritorial claim of the EU, despite its broadness, is rather legitimate and even part of a shared tendency among jurisdictions around the world to extend the reach of data protection laws. Second, the enforcement tools of the regulation. This work reveals that the EU may benefit from some direct enforcement tools such as representatives and international cooperation, but also, and more importantly, through indirect means. In particular, the EU may rely on the risk of reputational damage, the incentives to self-compliance, and the rules on data transfers to third countries.

Keywords: Data protection; GDPR; compliance; overseas data processing; extraterritorial scope; enforcement; international law; international cooperation

Recommended citation: Adèle Azzi, The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation, (2018) JIPITEC 126 para 126

A. Introduction

1 More than ever, any attempt to regulate data privacy has become highly complex and controversial.

2 The current features of data privacy have encouraged the Commission to reform the European Union (EU) data protection framework, but, at the same time, the very same features make this reform a real challenge.

3 First, data privacy ought to be protected as a fundamental right in the EU, under Article 8(1) of the Charter of Fundamental Rights and Article 16(1) TFEU. Since 1970, when the first data privacy act in the world was adopted in Germany, data privacy has developed in each Member State, then at the EU level, becoming the world's strictest and most influential data privacy regime.

4 Second, data have become a valuable and competitive asset, a currency, and even a commodity on its own. Facebook's motto: "It's free and always will be" is not exactly true. Row data have always had a commercial value for businesses, but the current techniques of data processing, in addition to the wider amount of accessible data, have made it become a key asset for targeting and developing a demand. The role of data in the development of the economy is recognized worldwide, in particular in the EU.[1]

5 Last, but not least, data privacy has acquired a transnational aspect. While, not a long time ago, the data controller, the data subject and the means used for data processing were often located in one country,[2] the development of international trade, the new technologies and the new corporate structures of multinational companies have increased the importance of the international processing and transfer of data. This new borderless environment does not give much credibility to data protection laws with a domestic territorial scope. A "territorial scope 2.0"[3] is now required.

6 Since 2010, the Commission has been working on the creation of a new EU data protection framework,[4] which until now, was mainly contained in the 1995 Data Protection Directive ("the directive").[5] Years of debate and heavy lobbying have led to the adoption of the General Data Protection Regulation (GDPR, "the regulation") of 27 April 2016, which took effect on the 25th of May 2018.[6]

7 Much noise is made around the obligations imposed by the GDPR on controllers and processors (who will be called "operators"), for the processing of the personal data of individuals located in the EU. Undoubtedly, it brings about substantial changes in comparison to the directive. Nonetheless, the biggest change surely lies in the new territorial scope of the data protection rules. Under Article 3 of the GDPR, operators who used to be entirely out of the reach of EU data protection rules, despite heavily processing EU data, will suddenly have to comply with the highest data protection standards in the world. However, does the EU and its Data Protection Authorities (DPAs) have the means to effectively apply the regulation outside its borders? Who are the overseas operators?

8 The focus is often placed on the social networks, email providers, or search engine operators based in the US; but a large part of the processing today also takes place in Asia, particularly China. Many EU citizens use Chinese products such as the Huawei's smart phones, the search engine Baidu, their cloud computing services, banking services, etc.

9 The efficient application of the GDPR on those large non-EU companies, as well as smaller ones, is said to be dependent on some specific factors: first, the legitimacy of the extraterritorial claim, and second, the enforceability of the claim,[7] knowing that the former will greatly condition the latter. Indeed, it is acknowledged that "*where it is morally justifiable, it is perilous for the target of the claim to ignore it, and where it is not morally justifiable, it is perilous for the [country] to make the jurisdictional claim*".[8]

10 In the light of these factors, this essay assesses the challenges faced by the new territorial scope of the GDPR, in particular by focusing on Article 3(2) which embodies its extraterritoriality by extending jurisdiction over activities and operators located

* LL.M. student at the London School of Economics.

1 Communication from the Commission "Building a European data economy", COM(2017) 9 final, January 2017.

2 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, 2016, Vol. 6, No. 3.

3 Merlin Gömann, *The new territorial scope of EU data protection law: deconstructing a revolutionary achievement*, Common Market Law Review, 54, pp. 567 – 590, 2017.

4 Communication from the Commission "A comprehensive approach on personal data protection in the European Union", COM(2010) 609 final, November 2010.

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31.

6 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) [2016] OJ L 119/1.

7 Dan Jerker B Svantesson, *Extraterritoriality and targeting in EU data privacy law: the weak sport undermining the regulation,* International Data Privacy Law, 2015, Vol. 5, No. 4, p. 233.

8 (n 7).

outside of the EU.[9]

11 If the contractual freedom of the parties shall not enable them to derogate from the GDPR by agreement,[10] the efficiency of its extraterritorial scope keeps facing several challenges. The very limited nexus of jurisdiction, which does not require any physical presence in the EU, the immaterial features of cyberspace and the particularly burdensome duty of compliance imposed on operators, are, all together, casting doubt on the actual enforceability of the GDPR on non-EU businesses. Article 3(2) is supposed to put an end to any attempt of circumvention of EU data protection rules, but such an objective might only be a *façade*.

12 In other words, to reuse the terms of an author, does the GDPR provide "bark jurisdiction", or "bite jurisdiction"?[11]

13 After an explanation of the extent of the extraterritorial claims of the GDPR (B.), this essay will assess the challenges that they face through two main angles: first, the legitimacy of the extraterritorial scope (C.); and second, its enforceability in the international online context (D.).

B. The extraterritorial aspirations of the GDPR: from a territorial to a destination approach

14 It is acknowledged that the wider the jurisdictional claim, the more reasonable it will be for other states to refuse to recognise it.[12] But in the borderless context of Internet, where should the line be drawn? How can a European data protection framework reconcile the desire to protect EU personal data and the legal certainty that is owed to foreign businesses?

15 Through the combined use of a territorial and a "destination" justification, Article 3 of the GDPR incorporates the extraterritorial claims already made by the courts under the directive (B.I), and then pushes the boundaries further (B.II).

I. The incorporation of previous solutions: the extraterritorial application of the directive

16 The scope of the directive should have followed a territorial approach, under which the EU data protection rules could only be applied to controllers that have a certain physical presence in the EU. However, this legal basis of application has been stretched and changed by the courts beyond recognition.

17 First, the directive applied when "*the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State*".[13] Thus, in principle, the directive could not reach a controller processing EU data entirely outside the EU, even if the controller had some establishments within the EU, unrelated with the processing activity. As soon as technological developments made it possible to process data at a distance, the scope of the directive could easily be circumvented, until the Court of Justice intervened. In the *Google Spain* case, the processing was carried out by Google Inc., the US based company, but it was made profitable through the activities of the EU establishment Google Spain. According to the Court, the economic link between the EU establishment and the US processing entity amounted to a processing carried out "in the context of the activities" of the EU establishment. Therefore, the US entity was bound by the directive when processing EU data in the US territory.[14] From now on, these mental gymnastics are not required anymore because Article 3(1) specifies that the EU rules apply "*regardless of whether the processing takes place in the EU.*"

18 Second, when the controller was not established in the EU, the directive would apply if, "*for purposes of processing personal data, [the controller] makes use of equipment (...) situated [in the EU]*".[15] At the time the directive was drafted, "equipment" probably referred to main-frame computers and servers. However, it has been extended so that the directive would apply to controllers without any physical equipment in the EU. The main extension was made by The Article 29 Working Party ("Art. 29 WP"), an independent EU advisory body on data protection. It considered the placing of "cookies" in personal computers in the EU as "making use of equipment" within the EU.[16] Under this interpretation, the user's PC is

9 See for a definition of extraterritoriality, (n 7), p. 227.

10 Maja Brkan, *Data Protection and Conflict-of-Laws: A Challenging Relationship*, EDPL 3/2016, pp. 333 – 334.

11 Dan Jerker B. Svantesson, *The Extraterritoriality of EU Data Privacy Law – Its theoretical Justification and Its practical Effect on U.S. Businesses*, (2014) 50 Stanford Journal of International Law, 53, p. 58.

12 (n 11), p. 94.

13 Directive 95/46/EC, Article 4(1)(a).

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

15 Directive 95/46/EC, Article 4(1)(c).

16 Article 29 Data Protection Working Party, 'Working Document on determining the international application of EU data protection law to personal data processing on

seen as "equipment". Moreover, it also considered JavaScript, banners and spywares as "equipment", in the sense of Article 4(1)(c).[17] With the regulation, this artificial concept of equipment is replaced by Article 3(2)(b), since the provision extends the scope of EU rules to the processing related to the "monitoring" of the behaviour of people in the EU.

II. The new and broader extraterritorial claims of the GDPR

19 The GDPR aims to protect the personal data of people located in the EU. However, a pure protective approach would bring uncertainty for foreign businesses. EU data may be found in a number of situations, sometimes unexpectedly. Hence, the Commission has drafted the regulation in a way which rather places emphasis on the conduct of the operator itself, following a "destination" approach. Actually, as we will see, the only difference lies on the better justifiability of the claim. In practice, it has almost the same effects as a protective approach, which would have been applied wherever EU data were processed.

20 Article 3(2) allows the application of the EU rules to non-EU operators who process the data of individuals in the EU in two situations: first, if it is related to the offering goods and services in the EU (B.II.1); and second, if it is related to the monitoring of the behaviour of people in the EU (B.II.2).

1. Offering of goods and services: "you are targeted if you target"

21 Under Article 3(2)(a), the regulation applies to non-EU operators where they process the personal data of individuals in the EU, in relation to the "*offering of goods or services*" to them, including free of charge. This is not an unusual basis for jurisdiction, but it raises some controversy in the internet world.

22 This basis for jurisdiction is not surprising. It is also found in Brussels 1 Regulation which provides that, as soon as the professional has directed by any means its activity towards the consumers domiciled in a certain Member state, those consumers cannot be deprived of the protective and non-derogable rules of the Member state[18]. It is the "targeting" logic, under which "you are targeted by EU law only if you target".[19]

23 The rationale, however, becomes more controversial in the context of online sales and worldwide accessible websites. In this context, one could ask in the case of "*who is targeting who in the transaction?*"[20] whether the consumer is specifically looking for the particular website? However, Recital 23 of the GDPR adds that the targeting should be "*apparent*". To assert such intention, the accessibility of the website may be combined with the possibility of ordering goods and services in the language or with the currency of one or more Member States or the mentioning of EU customers.[21] The case law under Brussels 1 also provides additional relevant factors of targeting such as "*the international nature of the activity, mention of itineraries from other Member States (...), mention of telephone numbers with an international code, (...), use of a top-level domain name other than that of the Member State in which the trader is established (...).*"[22]

24 In practice however, one may wonder whether the court will require an "active dis-targeting" on the part of the operator. In the US, under the targeting principle, a US court considered that it had jurisdiction over a Canadian website used by Americans, because the latter did not technically "prevent" access to its website by Americans who could access it by declaring that they were Canadian residents.[23] As Svantesson suggests, the use of geolocation technologies might be a solution, however access to this information always requires the consent of the user, even if not for monitoring purposes.

2. The monitoring of the behaviour of individuals located in the EU

25 Under Article 3(2)(b), the GDPR applies to non-EU operators who process the personal data of individuals in the EU where the processing is related to the monitoring of their behaviour, as far as their behaviour takes place in the Union. In light of this provision, what types of processing of EU data may actually fall out of the regulation? The answer is only very few.

---

the Internet by non-EU based web sites' (WP 56, 30 May 2002); see comments by Lokke Moerel, *The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?*, International Data Privacy Law, 2011, Vol. 1, No. 1.

17 Lokke Moerel, (n 16).

18 Regulation (EU) No 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, Art. 17(1)(c).

19 (n 2).

20 (n 2), p. 241.

21 GDPR, Recital 23.

22 Joined cases *Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG* (C-585/08) and *Hotel Alpenhof GesmbH v Oliver Heller* (C-144/09), §93.

23 *Twentieth Century Fox Film Corp v. iCraveTV*, Nos. 00-121, 00-120, 2000 WL 255989 (W.D. Pa. Feb. 8, 2000).

26 First, the concept of monitoring receives a particularly broad definition. There is "*monitoring" where "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 analysing or predicting her or his personal preferences, behaviours and attitudes.*"[24]

27 It follows that most of the processing of EU data will trigger the application of the GDPR, in particular when it is carried out by businesses. Nonetheless, it shall not apply to a non-EU entity which, for example, collects data on EU consumers in order to classify individuals based on their characteristics and obtain an aggregated overview of its clients without making any predictions about an individual.[25]

28 Secondly, the limits of the concept of "monitoring" is highly impacted by the definition given to "personal data". They include, but are not limited to, the user's personal preferences, interests, location or movements.[26] The regulation specifies that online identifiers like IP addresses and cookie identifiers can serve to profile natural persons[27] and thus be qualified as personal data. As a result, the monitoring does not even "mainly" concern social networks, email providers, or search engine operators, but impacts the vast majority of websites that collect the "click stream data" (surfing behaviour),[28] either through the use of cookies, ad banners or JavaScript.

29 In conclusion, Article 3(2) significantly increases the scope of EU data protection rules in a unilateral way, and to a greater extent than any other jurisdiction in the world has done until now. Even if it refers to the alleged voluntary conduct of the operator to justify the application of the regulation, in practice the application of the regulation almost "follows" the EU data. Given the sudden application of EU rules to many websites around the world, one may wonder on which legal basis does the regulation ground its legitimacy and authority.

C. The legitimacy and legal basis for an extraterritorial application of the GDPR

30 The Regulation amounts to a unilateral expansion of the application of European law to non-EU businesses. No one could deny that this expansion is justified by the borderless domain of the Internet, which in response requires also a borderless application of the law. In a way, there is no doubt that effective data protection on the Internet does not get along with a domestic scope of application. Nonetheless, the EU dares to go much further than any other state on this aspect, and with the highest level of standards in the world. It is not only challenging state sovereignty, but also imposing a particularly heavy burden of compliance on overseas businesses, not to mention the high costs of the administrative fine.

31 On which legal basis can the EU unilaterally extend its authority over non-EU entities and justify or legitimate these new self-acquired powers in the eyes of the world?

32 The unilateral expansion of jurisdiction out of the borders is not a rare phenomenon and has been carried out by most countries, in particular in relation to criminal matters. Such extraterritorial claim must however respect some specific rules. Indeed, when doing so, jurisdictions, including the EU and its institutions,[29] are bound to respect public international law. It is therefore necessary to review the conditions under which public international law legitimates an extraterritorial claim, knowing that the outcome of this assessment may either seriously challenge such expansion or, on the contrary, support it and deem it hardly questionable.[30]

I. The identification of the international rules governing extraterritorial claims

33 Article 29 Working Party has held that cross-border cases in data protection law is "a general question of international law"[31]. In general, there is a principle, stated by the seminal case *Lotus*, that states have "*a wide measure of discretion (...) to adopt the principles which it regards as best and most suitable*".[32] Nonetheless, the fundamental principles

24 GDPR, Recital 24.

25 Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01), p. 7.

26 GDPR, Art.4.

27 GDPR, Recital 30.

28 Lokke Moerel, (n 16).

29 Case C-366/10 , *Air Transp. Ass'n of Am. and Others v. Sec'y of State for Energy and Climate Change*, 2011, §101.

30 (n 11), p. 76.

31 Article 29 Data Protection Working Party, (n 16), p. 2.

32 PCIJ, *SS Lotus, (France v Turkey)*, PCIJ Reports, Series A, No 10, p. 19 (1927).

of state sovereignty and non-interference require some limitations.[33] Such limitations are not easy to draw in light of the sometimes very creative grounds invoked to justify jurisdiction. One may however refer to "the most authoritative outline" of the sources of international law, provided by Article 38 of the Statute of the International Court of Justice.[34] Under this article, the legitimacy of extraterritorial claim may be assessed in light of "*international conventions [...] establishing rules expressly recognized by the contesting states; international custom, as evidence of a general practice accepted as law; (and) the general principles of law recognized by civilized nations [...]*".

34 Regarding international conventions, no international treaty is directly related to data protection, so it may not be the most relevant factor to consider. Admittedly, the principle of privacy protection is clearly enunciated at least by two interventional conventions, i.e. the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). It does not however provide guidance to assess the legitimacy of the scope of the GDPR.

35 Therefore, the focus will be placed, first, on international custom, which will indicate the degree of acceptance of these claims (C.II.) and second, the general principles of law recognized by civilized nations, which will allow for a comparison with other states' extraterritorial claims in data protection (C.III.).

II. The limited support of international customs

36 To consider a jurisdictional basis as an international custom, it is required to satisfy conditions of duration, uniformity and constancy of the practice, and the authority of the jurisdictional basis will vary accordingly.

37 To begin with, the "territorial principle" undoubtedly constitutes an international custom as it is the most universally accepted jurisdictional basis. It consists, merely, in determining jurisdiction by reference to the place where the offence is committed[35].

38 A more controversial basis, although increasingly common, is the "effects doctrine". It bases jurisdiction upon the fact that a conduct which took place outside the state has effects within the state.[36] It is particularly relevant in antitrust law and has been recognized, for example, by the US Supreme Court which stated that "*acts done outside a jurisdiction, but intended to produce and producing detrimental effect within it, justify a state in punishing the cause of the harm as if he had been present at the effect*".[37] However, the problem with this basis, as noted by Kuner, is that it is "*open-ended*", in particular in a globalized economy, where "*everything has an effect on everything*".[38]

39 Finally, jurisdiction is sometimes based on the passive personality principle. This ground, which determines jurisdiction by reference to the nationality of the victim, does not reach the statute of international custom as it remains a highly controversial basis.

40 In light of these grounds, it seems that Article 3(2) of the GDPR is based on the "effect doctrine", which remains a controversial basis of jurisdiction. The GDPR places the focus on the location of the potential harmful effects and discards the location of the processing of the operator. It is worth noting that, initially, the 2012 draft of the GDPR founded jurisdiction on the passive personality principle, applying the EU rules to EU *residents*. In the final version, the term "resident" has disappeared from Article 3 and has been replaced by the vague terms "data subjects who are in the Union".

41 While the assessment of international custom allows us to identify the approach chosen by the GDPR and provides a first overview of its level of acceptance, further details are provided by the General Principles of Law.

III. Legal basis in regard of the General Principles of Law Recognized by Civilized Nations

42 This source is subsidiary to customary law and consists in mapping the domestic laws of states and, more specifically, their respective jurisdictional scope in terms of data protection. Without going through all domestic data protection laws, the assessment of a few regimes is quite indicative of the degree of legitimacy that may be recognized by the GDPR, and hence its authority.

43 Regarding data privacy, extraterritorial claims become widespread. For example, in Australia, the 1988 Privacy Act applies to any organisation

33 Christopher Kuner, *Data protection law and international jurisdiction on the Internet (Part 1)*, International Journal of Law and Information Technology, Oxford University Press 2010, p. 186.

34 (n 11), p. 76.

35 Introductory Comment to the *Draft Convention on Jurisdiction with Respect to Crime,* 29 AM. J. Int'l L. 439, p. 455.

36 (n 11), p. 82.

37 *Strassheim v. Daily*, 221 U.S. 280, 285 (1911).

38 (n 33), p. 190.

or small business operator with an "Australian link", in particular where such entity carries on business in Australia.[39] In Singapore, the Personal Data Protection Act of 2012 applies to organisations collecting personal data from individuals in Singapore whether or not the organisation itself has a presence in Singapore.[40] In the US, the Children's Online Privacy Protection Act (COPPA) applies to foreign-based websites that are either directed to children in the US or which knowingly collect personal information from children in the US. This formulation inevitably resembles the scope of the GDPR.

44 Reference can also be made to other fields, in particular to the US. The US is indeed generally not reluctant to extend the territorial scope of their law, and the best illustration is provided by the US Foreign Corrupt Practices Act ("FCPA").[41] Its scope has been extended by the courts to issuers of securities on the US markets, and even acts of bribery committed through the use of a US-based email provider.[42] This fact is not only relevant to identify general principles of law, but also to show that the US, despite the important impact of the GDPR on their businesses, are not in the best position to object to such territorial scope.

45 In consequence, while the international custom was displaying rather shy support for the scope of the GDPR, the General Principles of Law reveal a tendency to broaden the reach of data protection laws. Many countries seem to acknowledge the need to apply the data protection rules outside their borders. However, should the new scope of application be considered as "bark jurisdiction or bite jurisdiction"?[43]

D. "Bark jurisdiction or bite jurisdiction": the enforcement issues

46 The capacity of enforcement faces a lot of difficulties in an environment which combines non-physical aspects (cyberspace) with extraterritoriality. As noted by Goldsmith and Wu, "*with few exceptions, governments can use their coercive powers only within their borders and can control offshore Internet communications only by controlling local intermediaries, local assets and local persons*".[44] Besides, obstacles against enforcement can arise at several stages of the procedure, from the beginning of investigations to the application of a sanction. However, surprisingly, the literature related to the enforcement of the GDPR in non-EU countries is rare, if not non-existent. Although it seems to be an unspoken issue, it has appeared in several guides drafted by law firms that the enforcement of the GDPR over non-EU companies remains "unlikely".

47 After a brief description of the related powers of supervisory authorities (D.I.), this essay will examine the different solutions which may beat the odds and preserve the efficiency of the GDPR and the authorities' powers in non-EU cases. They comprise of direct means of enforcement (D.II.) and indirect ones (D.III.).

I. The broad investigative and corrective measures in the hands of supervisory authorities

48 In the GDPR, the investigative powers and ability to sanction are both extremely broad.

49 A supervisory authority is allowed to order the operator to communicate information, to carry out data protection audits, to obtain access from the operator to all personal data necessary for the performance of its tasks, and to obtain access to any premises of the operator, including data processing equipment.[45]

50 In terms of corrective powers, the authority can, among other measures, issue a warning to an operator, impose a temporary or definitive limitation such as a ban on processing, order the rectification of erasure of personal data and impose an administrative fine.[46] The fine goes up to 4% of the total worldwide annual turnover for the most serious breaches, which actually includes most of the substantial obligations imposed by the regulation. It applies to violations of the requirement of consent and all the basic principles for processing, the data subject's rights such as the "right to be forgotten", the rules on data transfer to third countries, and for the non-compliance with an investigative or corrective measure.

39 Privacy Act 1988, Section 5B, paragraph 3(b), accessible on <https://www.legislation.gov.au/>.

40 <https://www.dlapiperdataprotection.com/index.html?t=law&c=SG>.

41 Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. ("FCPA").

42 French National Assembly Information Report n°4082, 5 Oct. 2016, on the Extraterritoriality of American laws.

43 (n 11), p. 58.

44 Jack Goldsmith and Tim Wu, *Who controls the internet?, Illusions of a Borderless World*, Oxford University Press, 2006, p. 159.

45 GDPR, Art.58(1).

46 GDPR, Art. 58(2).

II. The possible direct means of enforcement of the GDPR against non-EU operators

51 Direct solutions of enforcement involve the role of representatives, the cooperation between jurisdiction, and possible international measures against non-compliers.

1. The role of representatives

52 A response to the difficulties of international enforcement may be found in the role of representatives.

53 Under Article 27, any operator which is subject to Article 3(2) and does not have an establishment in the EU shall designate a representative in the EU, in one of the Member States in which the data subjects are located.[47] Operators may designate only one representative, a legal entity or an individual for the whole territory of the EU. Representatives differ from Data Protection Officers ("DPOs"), even though their role overlaps in some ways. The role of the representative, as its name implies, is to represent foreign operators with regard to their obligations and create a point of contact between them and the EU authorities. More specifically, the representative is required to cooperate with the authorities regarding any action ordered to ensure compliance with the regulation.[48]

54 However, its role may go beyond this function and actually elevate the representative as a primary tool of enforcement. Indeed, recital 80 provides that the designation of such a representative does not affect the responsibility or liability of the operator, but adds that the representative "*should be subject to enforcement proceedings in the event of non-compliance by the controller or processor*". In a previous draft of the regulation, this statement was made under Article 27, before being displaced to the preamble of the regulation. Unfortunately, the regulation does not provide any details on the enforcement mechanisms in question.

55 There is much controversy as to whether a representative may incur some sort of liability, in addition to the operator, and no guidance has been issued by the Art. 29 WP. Meanwhile, as the first Member State to have implemented the regulation, Germany has interpreted this provision law as enabling civil law proceedings to be directed against the representative.[49] Further, in a recent case against WhatsApp, held under the directive, the Netherlands has considered that the DPO could incur liability in case of non-compliance with the directive,[50] despite this not being specified by the directive. In response, WhatsApp claimed that it could not find any officer ready to endorse such liability, but the "impossibility" argument has been rejected. The Dutch court added that the parties could agree in contract to indemnify the officer in case of liability. Besides, the IAPP, a non-profit organisation which share best practices for privacy management issues, has also interpreted Article 27 of the regulation in this sense: "*it seems likely the EU representative would be required to at least initially incur the legal and other costs for addressing enforcement actions and be responsible for paying administrative fines and damage suit awards*".[51]

56 From those observations and considering the influence that may have the first implementation law on other Member States, there is a real possibility for representatives to be subject to enforcement measures. Of course, the law would be more effective if such power of coercion could be exercised locally. Besides, it would reduce the costs inherent to cross-border litigation.

57 However, a number of objections temper this possibility. First, as it was claimed by WhatsApp, operators might encounter a real difficulty in finding a representative eager to incur a potentially significant liability. Second, a representative may not actually have much influence over the foreign operator and may not have sufficient financial or material means to deal with the sanctions. Finally, even though the obligation to appoint a representative is sanctioned by a fine of up to 2% of the global turnover, there might well be some operators who decide to ignore it and not respond to any sanctions.

58 It follows that the existence of representatives in the EU territory will probably facilitate the enforcement of the regulation in some cases, but can only be seen as one the possible means to achieve an effective enforcement abroad.

47 This obligation does not apply to processing that is occasional, does not involve sensitive data and is unlikely to result in a risk to the rights and freedoms of natural persons.

48 GDPR, Recital 80 and Art. 31.

49 Section 44(3) of the Federal Data Protection Act of 30 June 2017 (Federal Law Gazette I p. 2097).

50 Administrative Court of The Hague, 22 November 2016, SGR 15/9125.

51 International Association of Privacy Professionals (IAPP), <https://iapp.org/news/a/how-do-the-dpo-and-eu-representative-interplay/>.

2. The cooperation between jurisdictions

a.) The cooperation for investigation measures

59 Under international law, it is prohibited for a state to perform an act on foreign territory when it falls within the exclusive competence of the foreign state officials, such as investigation. The consent of the foreign state must be obtained, regardless of the consent of the parties.[52] This rule is shared by every country, including China which codified it under Article 277 of CiPL.

60 Some authors mention the possibility of resorting to international cooperation agreement, such as agreement of mutual legal assistance (MLA). Currently, the vast majority of those treaties are related to criminal cases.

61 Regarding data protection, some punctual authorisations have been given. It happened for the first time in 1996, when the German DPA obtained the consent of Citibank to conduct an on-site audit of the data processing facilities of its US subsidiary, which had received the credit card data of German customers.[53] A further example is given by the Spanish DPA, which also conducted an audit on the processing equipment of a data recipient in Colombia, on the basis of a contractual clause authorising such an investigation.

62 These cases raise the question as to whether the cooperation could actually be organised through contractual clauses. Actually, some standard contractual clauses for data transfers outside the EU already contain a prior authorisation given to the relevant DPA.[54] However, as noted by Christopher Kuner, the consent of the relevant government authorities will always be required and, according to him, was obtained by the German and Spanish DPAs in the cases mentioned.[55]

63 An EU DPA may also overcome the reluctance to consent of the foreign authorities by asking its DPA to conduct the measures itself, on behalf of the EU DPA, but an agreement would have to be reached as to the costs incurred by the operation.

52 Christopher Kuner, *Data protection law and international jurisdiction on the Internet (Part 2)*, International Journal of Law and Information Technology, Oxford University Press 2010, p. 232.

53 (n 52), p. 233.

54 See Commission Decision 2001/497 of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, 2001 O.J. (L 181/19).

55 (n 52), p. 233.

b.) The cooperation for the enforcement of a judgment or administrative decision

64 To understand the possibilities of enforcement of judgments from EU courts or DPAs, it is necessary to briefly recall some principles of international law.

65 To be efficient abroad, a judgment needs to be *recognized* and *enforced* by the foreign court. The basic theories on which it is done are, first, the "comity" theory, which often requires reciprocity or a treaty between the states, and second, the "obligation theory", under which it would be fair to the parties to enforce it.

66 In China, in theory, recognition and enforcement of foreign judgment ("REJ") are possible if there is, among other conditions, a treaty of mutual judicial assistance or reciprocity.[56] Until recently, it was almost impossible to obtain REJ absent a treaty of mutual judicial assistance, which is rare and usually focused on criminal cases. However, lately, Chinese courts have shown more willingness to enforce foreign judgment on the basis of reciprocity and have adopted a pro-active attitude in triggering the reciprocity cycle.[57]

67 Beyond comity and reciprocity, the existence of shared values of privacy protection with the foreign jurisdiction and the legitimacy of the extraterritorial claim will significantly impact the likelihood of foreign enforcement. The more limited the nexus for jurisdiction is, the more likely it is that the foreign jurisdiction will not enforce the decision.

68 Jurisdictional claims regarded as illegitimate in light of those two factors may even lead to the adoption of a "blocking statute". Such legislation may forbid the production of evidence or any documents in foreign proceedings, prohibit compliance with orders of foreign authorities, etc.[58] As extreme as it may sound, it is actually quite common.[59] For example, in the US it may be unlikely to obtain the enforcement of a decision relating to the GDPR's "right to be forgotten", which affects freedom of

56 Article 282 of China's Civil Procedure law.

57 Wenliang Zhang, *Sino-Foreign Recognition and Enforcement of Judgments: A Promising "Follow-Suit" Model?*, Chinese Journal of International Law, Volume 16, Issue 3, 1 September 2017, pp. 515 – 545.

58 Senz and Charlesworth, *Building Blocks: Australia's Response to Foreign Extraterritorial Legislation*, 2 Melb. J. Int'l L. (2001), p. 27.

59 See for instance in Australia, Section 7 of the Foreign Proceedings Act 1984 (Cth); in Switzerland, Art. 271 of the Swiss Criminal Code; in the EU, Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom (which has been recently reactivated in response to the US embargo on Iran).

expression, protected by the First Amendment. Indeed, the Congress has already adopted a blocking statute concerning what they see as "libel tourism": it makes mandatory the non-recognition of foreign defamation judgments where a US Court would have reached a different judgment under the First Amendment.[60]

69 In conclusion, cooperation with foreign jurisdiction may be relied on for the enforcement of the GDPR outside Europe to the extent that the jurisdictional claim is reasonable and legitimate (and with the consent of the State for investigation measures). It follows that it would probably require more than the mere utilisation of cookies to enforce a judgment abroad through the sole means of international cooperation.

3. Other possible direct measures against the operator

70 Of course, when an operator is not established in the EU but possesses assets in the EU, the question of enforcement is not an issue anymore, even though it may require a preliminary asset-freezing order to prevent it from taking its property out of the EU once the action is brought forward.

71 When the foreign operator does not possess assets in the EU, or sufficient assets, other measures might however impact it sufficiently to force it to comply with the DPA's decision.

72 As recalled by Svantesson, the government may introduce "market destroying measures" to penalise the operator. It consists of prohibiting the party to trade within the jurisdiction or make the debts owed to that party unenforceable within the jurisdiction.[61] The impact of this measure depends on the importance of the market for the operator.

73 There are other creative ways of affecting its commercial interests to force it to comply. A DPA could obtain a court injunction against the local business partners that are indirectly using the processed personal data. A court injunction could also allow the blocking of the websites of the operator or its partners, or the associated internet connections (*via* injunctions applied to internet service providers).[62]

60 (n 11), p. 95; 28 U.S.C. §4102 (2012).

61 (n 11), p. 98.

62 <https://medium.com/mydata/does-the-gdpr-apply-in-the-us-c670702faf7f>.

74 In spite of those options that should allow enforcement of the GDPR in serious cases of non-compliance, it is undeniable that those measures do not entirely fill the gap between the scope of the GDPR and the scope of its enforceability. The efficiency of the regulation should be enhanced by indirect but more reliable means of enforcement.

III. Indirect means of enforcement of the GDPR against non-EU operators

1. The reputational impact

75 As noted by a law firm, in the *Google Spain* case, "*Google's prompt compliance with the Google Spain decision could suggest that companies will be loath to risk the reputational damage incurred from refusing to comply with a data protection enforcement notice, rendering the practical difficulties of enforcement irrelevant.*"[63] The reputational image will always play a role as soon as the company's failure to comply may be mediatised and the claim is morally justifiable.

76 Actually, the reputation is so crucial that it may even have the capacity to broaden the scope of the GDPR. Facebook is currently facing this issue since its declaration in April 2018. Mark Zuckerberg announced that Facebook would apply "*in spirit*" the GDPR to the rest of the world. It has resulted in a change to its terms and conditions so as to remove from the Irish jurisdiction the 1.5 billion non-EU users (70% of the members) to the US jurisdiction. It triggered a global uproar.[64] The Transatlantic Consumer Dialogue has publicly written to Facebook: "*We write to you on behalf of leading consumer and privacy organizations (...) to urge you to adopt the [GDPR] as a baseline standard for all Facebook services. There is simply no reason for your company to provide less than the best legal standards currently available to protect the privacy of Facebook users.*"[65]

77 Although this is the case for companies subject to the pressure of public opinion, the reputational damage will be unlikely to raise great concerns for smaller non-consumer businesses.[66]

63 Slaughter and May, *New rules, wider reach: the extra-territorial scope of the GDPR*, June 2016.

64 <http://www.bbc.co.uk/news/technology-43822184>.

65 <http://tacd.org/tacd-calls-on-facebook-to-adopt-same-privacy-standards-for-all-consumers-and-give-details-on-how-to-congress/>.

66 (n 63).

2. Self-compliance: a comprehensive enforcement at low cost for DPAs

78 The GDPR encourages self-compliance and the adoption of codes of conduct by operators subject to the regulation, but also by their business partners.[67]

79 The incentives to be self-compliant are again partly related to the protection of the company's image. Indeed, the regulation provides that the codes of conduct will be made available to the public by any means and encourages the establishment of certification mechanisms to demonstrate the compliance of the operator with the GDPR.[68]

80 From a practical view, it may also ease the enforcement of the GDPR since it should provide to DPAs a useful insight as to how the operator processes data and what sort of mechanisms can allow it to comply with the regulation.

81 The adoption of compliance programme is therefore another way to enhance the efficiency of the regulation, at a lower cost for EU authorities.

3. The rules of data transfer to third countries, a minimal safeguard

82 Similarly to the directive, under the Chapter V the regulation provides rules applying to the transfer of personal data to third countries. Mainly they require an "adequate" level of protection in the third country.

83 While these rules made sense under the restrictive territorial scope of the directive, one may wonder why they are still necessary considering the new (extra)territorial scope of the regulation. This co-existence is even more surprising since data transfer requirements are minor compared to Article 3, which imposes a full compliance to the regulation.

84 To illustrate the incoherence, we may take the example of an EU consumer who buys a product on a U.S. website, to be delivered to the UK. In this simple operation, the consumer will have entered its credit card details on a U.S. website, and the performance of the sale operation is likely to involve third parties who will receive some kind of personal data from the consumer, such as the billing or delivery address. Besides, it is very likely that the website will have set up cookies to track the consumer. Often, the information collected by the cookies is then transferred to a third party, such as Google Analytics, the web analytics service provided by Google.

85 In this very simple example, there are multiple occasions on which a DPA may characterize a data transfer. For instance, where a web analytics service has no direct link with EU consumers but processes their data, should it respect the whole regulation under Article 3(2)(b) or should it only be subject to adequacy rules? It is very likely that a DPA would make it fall under the entire regulation, even though the operation involved an international data transfer.

86 This demonstration aims to reveal that data transfer rules safeguard, in a way, the efficiency of the GDPR. While it is acknowledged that the GDPR will not always be individually enforceable against foreign operators, data transfer rules fill the gap through a general guarantee that, at least, an *adequate* level of protection in the third countries is applied. This is even more likely with regard to the absence of a definition of "data transfer" in the regulation, and hence its flexible application.

87 Consequently, Chapter V of the regulation is an indirect way of preserving the efficiency of the data privacy principles underlying the regulation.

E. Conclusion

88 In light of the international context and other domestic laws, the extraterritorial scope of the GDPR cannot be considered as an exception. It is part of a global trend to extend the scope of data protection laws to make them reflect the borderless nature of the Internet. However, the EU distinguishes itself by concurrently applying a very limited nexus for jurisdiction with, not only a heavy burden of compliance - in particular for small businesses - but also a substantial level of administrative fines.

89 Other examples of law, such as the US FCPA against corruption, demonstrate that a law can be efficient even with an extremely limited basis for jurisdiction. However, to succeed in subtracting billions of dollars from European companies, the US does not use "traditional" investigation and enforcement measures. As it is asserted in an official report from the French National Assembly, the enforcement in those conditions is made possible through the action of the FBI, for which the fight against corruption is its second priority.[69] Of course, in such circumstances, all the obstacles for investigation, such as the consent of the local authorities, are removed.

90 However, for the GDPR to apply through conventional investigation measures, and with a limited nexus for jurisdiction, a number of obstacles remain. This

67 GDPR, Art.40(1) and (3).

68 GDPR, Art.40(11) and 42(1).

69 French National Assembly Report, (n 42).

essay has shown, nevertheless, that the EU rather benefits from the "legitimacy" of the extraterritorial claims and is equipped with the relevant tools to enforce it abroad. That being said, it is necessary to develop those instruments further.

91 Besides, for those who remain convinced that the EU is not capable of effectively enforcing the GDPR outside Europe, it must be noted that unenforceable extraterritorial claims might still have some interests. Indeed, it is actually acknowledged by several jurisdictions with extraterritorial data protection laws that such laws - despite difficulties of enforcement - stand as a deterrence for overseas undertakings to engage in illegal processing and have the merit to "*provide consistent treatment for local vis-à-vis overseas organisations*".[70] As stated by Svantesson, even though a law that lacks the means to be enforced may undermine the legal system, "*morally justifiable law, including morally justifiable law that cannot be enforced, has a quality that cannot, and should not, be ignored*".[71]

70 Public Consultation Issued by the Ministry of Information, Communications and the Arts of Singapore *Proposed Personal Data Protection Bill* (19 March 2012) p. 6.

71 (n 11), p. 59.