the SPANISH YEARBOOK of INTERNATIONAL LAW

The extraterritorial application of European Union Data Protection Law

Ana GASCÓN MARCÉN*

Abstract: This paper will examine the extraterritorial application of European Union Law regarding the Internet in three particular cases that exemplify a current trend and make apparent the advantages and challenges of this approach. The examples relate to the protection of personal data and, in particular, the scope of the General Data Protection Regulation, the right to be forgotten and cross-border access to electronic evidence. The paper will end with some recommendations on how to avoid the problems that the extraterritorial application of the law in this field may entail.

Keywords: Personal data protection electronic evidence extraterritoriality human rights right to be forgotten

(A) INTRODUCTION

Internet was at its inception a virtual space, a way to communicate regardless of borders. Nevertheless, we are far from the first utopian approaches of John Perry Barlow that in his *Declaration of the Independence of Cyberspace* famously proclaimed "Governments of the Industrial world, (...) I come from Cyberspace, (...) on behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather". Internet and the activities anyone undertake on it should be subject to the law as any other human endeavour. The question is which law and if it is possible to build walls around it.

The European Union (EU) must regulate matters such as protection of copyright, the fight against terrorism, commerce, etc. However, this gets complicated when it involves the Internet, a medium that by its very nature is global.[1] The conception of Law and its application are traditionally linked to the territory for reasons of sovereignty and effectiveness. This has not prevented other states from taking measures that tend to fragment the Internet[2] as the *Great Firewall of China* or Russia's new Law that hopes to reclaim a "sovereign Internet".[3] Nevertheless, an organization like the EU based on the values of the protection of human rights, the rule of law and democracy cannot rely on such kind of measures that seek to create walls and contribute to censorship.

Article published on 31 December 2019

* Lecturer of Public International Law, University of Zaragoza. Mail: angascon@unizar.es.

1 The problem of laws related to the Internet and jurisdiction has been discussed for more than twenty years but it is still unresolved. See D. R. Johnson and D. Post, "Law and Borders - The Rise of Law in Cyberspace", 48 *Stanford Law Review* (1996), 1367-1402 [doi: 10.2307/1229390]; J. R. Reidenberg, "Lex Informatica", 76(3) *Texas Law Review* (1998), 553-593; and D. C. Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces", 4 *Michigan Telecommunications and Technology Law Review* (1998), 69-103.

2 This phenomenon is defined as "splinternet" or the "balkanization" of the Internet.

3 See K. Idrisova, "Explainer: Russia's drive for a sovereign internet", *BBC Monitoring's*, published on 12 February 2019, accessed on 19 July 2019.

 DOI: 10.17103/sybil.23.28

The EU has problems in making its legislation effective and companies that offer their services in the EU should not be able to escape from its regulations just by placing their servers in third countries, but the EU can neither simply impose its own rules at a global level interfering with the jurisdiction of other states. Laws with an extraterritorial application are not new,[4] but they are gaining traction in all the fields related to the Internet.[5]

This paper will examine the measures taken or proposed in the EU in specific fields related to the protection of personal data as the scope of the General Data Protection Regulation (B) or the right to be forgotten (C) and cross-border access to electronic evidence (D). These are only three particular areas but they are examples of a broader trend in the EU and make apparent the advantages but also the problems of applying laws extraterritorially.

(B) THE SCOPE OF THE GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR)[6] has a marked extraterritorial impact since it applies to millions of companies located outside the EU. The GDPR, as stated in its Article 3, applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU (regardless of whether the processing takes place in the EU). In addition, it also applies to the processing of personal data of persons who are in the EU by a controller or processor not established in it, where the processing activities relate to the offering of goods or services[7] to persons in the EU, or the monitoring of their behaviour.[8] As we can see, the first part follows a subjective territoriality principle, taking into account who processes or controls the data, while the second adds a passive personality principle following the target of such actions.

---

4 For a thorough study of some examples to inform EU policy-making, see R. Dover and J. Frosini, *The Extraterritorial Effects of Legislation and Policies in the EU and US* (European Union, Brussels, 2012) [doi: 10.2861/75161].

5 See Internet Society, *The Internet and extra-territorial effects of laws* (Internet Society, 2018). In this concept paper (at 1), the Internet Society warns that "decision-makers in many states are imposing rules that spill over onto the Internet elsewhere, hamper innovation, deter investment in their own countries and risk creating new digital divides that disadvantage their own citizens."

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), OJ 2016 L 119/1.

7 Recital 23 GDPR helps to clarify this concept: "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."

8 Recital 24 GDPR helps to clarify this concept: "in order to determine whether a processing activity can be considered to monitor the behavior of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviors and attitudes."

 DOI: 10.17103/sybil.23.28

Companies have a huge incentive to abide by the GDPR because in case of a serious violation of it, the offender can be subject to fines up to 20 000 000 €, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (Article 83 GDPR).

The goal of this ample territorial scope is that the protection offered by the GDPR "travels" with the personal data wherever it goes in a globalized society where data crosses borders with a simple click. Offering protection only for data processing taking place within European borders would be meaningless in a globalized society. This measure also seeks to offer a level-playing field for European companies not creating a stricter regulation that would create burdens only for them. The extraterritorial application of the GDPR means that any company wanting access to the European market for offering its services and goods and dealing with "European" personal data in the process should abide by these rules.

Nevertheless, the GDPR has been harshly criticized because, with the number of businesses that fall under these criteria worldwide, it is easier for big firms to adapt to it while it is very costly for small and medium enterprises.[9] In addition, data protection authorities in the member states have limited resources, so Svantesson argues that "as there clearly will be more foreign businesses failing to comply with the GDPR than there are resources to investigate them, the actual application of the GDPR will necessarily be arbitrary, which arguably undermines the legitimacy of any enforcement actions taken."[10] Although Azzi considers "the EU rather benefits from the "legitimacy" of the extraterritorial claims and is equipped with the relevant tools to enforce it abroad"[11]. Hert and M. Czerniawski add that "this approach, although not without drawbacks and challenges to state interests and individual rights (...) solves one of the biggest problem European data protection law currently faces, which is lack of jurisdiction over third country's data controllers processing substantial numbers of EU data subjects' data."[12]

The problems are manifold and the critics have good reasons to be concerned, but the difficulty to ensure the application of the GDPR or the lack of resources for it cannot make us aim for lower standards of protection of fundamental rights,[13] even if the EU has to be mindful of the problems and challenges and strive to improve them.

The European legislators were quite conscious that the exterritorial application of laws could have undesirable impacts. The very GDPR in its recital 115 states that the extraterritorial application of some laws, regulations and other legal acts "may be in breach of international law and may impede the

---

9 See M. Scott, L. Cerulus and L. Kayali"Six months in, Europe's privacy revolution favors Google, Facebook", *Politico.eu*, published on 23 November 2018, or M. Scott, L. Cerulus and S. Overly, "How Silicon Valley gamed Europe's privacy rules",*Politico.eu*, published on 22 May 2019, both accessed on 19 July 2019.

10 D. J. B. Svantesson, "European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments", 9 (2) *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2018), 113-125, at para. 30.

11 A. Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation",9 (2) *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2018), 126-137, at para. 90.

12 P. de Hert and M. Czerniawski, "Expanding the European data protection scope beyond territory: Article 3 of the General Data. Protection Regulation in its wider context", 6 (3) *International Data Privacy Law* (2016), 230-243, at 230 [doi:10.1093/idpl/ipw008].

13 Art. 8 of the Charter of Fundamental Rights of the EU recognizes personal data protection as a fundamental right.

 DOI:10.17103/sybil.23.28

attainment of the protection of natural persons ensured in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met." The GDPR states its own extraterritorial application but precludes that of foreign laws in many cases.

For the extraterritorial application of a law, it is essential to find a substantial connection to avoid the risk of overregulation. Article 3 of the GDPR achieves this, even if its "targeting test" will need refinement by the case law of the Court of Justice of the EU.

Another key element is that the GDPR will enhance the fundamental rights of Internet users. It will have positive effects for European users but also for the ones outside EU borders as foreign companies who improve their personal data protection standards may decide to apply the enhanced standards worldwide. In addition, European data protection law has a spill over effect that makes that other states tend to converge with it (especially if they want a decision of adequacy of the European Commission).

A universal international treaty to deal with these matters would be even better. However, the United Nations could not reach such outcome and the only hope in this sense is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe. Nevertheless, this one is also limited, even if its scope goes far beyond Europe with Argentina, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia or Uruguay as state parties.

(c) The scope of the "right to be forgotten"

An issue that merits a particular approach in this field is the controversial "right to be forgotten". The Court of Justice of the EU in the case *Google Spain*[14] created a kind of "right to de-referencing", based on the right to the protection of personal data. It ruled that the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages when the data subject makes such a request,[15] even if some exceptions have to be considered, for example, when the information has public interest. This right has been widely criticized because it places such decisions in the hands of Internet intermediaries instead of judges and because it creates conflicts with the right to freedom of expression and the right to information.[16] Nevertheless, the GDPR

[14] Judgment of the CJEU (Grand Chamber) of 13 May 2014, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12. ECLI:EU:C:2014:317.

This case already presented some questions about the territorial application of EU personal data protection law. The Court ruled that Directive 95/46 was "to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State."

M. Gömann, in "The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement" 54 (2) *Common Market Law Review* (2017) 567 – 590, argues that the broadening of the scope of the GDPR was not as revolutionary as many believe as it was largely foreshadowed by the Court of Justice's judgment in this case.

[15] Because the information may be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine.

[16] See M. J. Oghia, *Information Not Found: The "Right to Be Forgotten" as an Emerging Threat to Media Freedom in the Digital Age* (CIMA Digital Report) published on 9 January 2018, accessed on 19 July 2019.

 DOI: 10.17103/sybil.23.28

enhanced it creating a "right to erasure" in its article 17.

Google does not apply the de-referencing of the controversial content globally to all its domains, but geo-blocks the requests for such information coming from the EU only. The French National Commission for Information Technology and Freedoms (CNIL) considered that this was not enough because the rights of Europeans were not effectively protected and sanctioned Google, which appealed the 100 000€ fine. A decision on the preliminary ruling before the Court of Justice of the EU is currently pending.[17]

The French Council of State asked whether a search engine is required, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by it so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester's name is conducted, and even if it is conducted from a place outside the territorial scope of the Directive 95/46;[18]or a search engine is only required to remove the links at issue from the domain name corresponding to the state in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the member states of the EU. The French Council of State also asked if the search engine operator is required to remove the results using the "geo-blocking" technique, from searches conducted on the basis of the requester's name from an IP address deemed to be located in the state of residence of the person benefiting from the "right to de-referencing", or even, more generally, from an IP address deemed to be located in one of the member states subject to Directive 95/46, regardless of the domain name used by the internet user conducting the search.

The simplified question would be if Google has to de-reference the controversial result worldwide or is it enough to limit it to the queries coming from the EU using geo-blocking. It is important here to underline that we are speaking about a different kind of exterritorial application of the law as the one explained in the previous section. In the case of the scope of the GDPR, the question was who has to abide by it, in the present case the question is not who but how. It is clear that Google has to abide by EU Law; the question is which should be the scope of the compulsory de-referencing.

The CNIL has strong arguments against limiting its application to requests to access content coming from the EU. Its President has explained that not to apply it worldwide "would be to empty the Europeans' rights of their substance and to consider that the scope of a fundamental right is variable in geometry, depending not on the one who exercises it but on the one who looks at the results."[19] In addition, this option could be easily circumvented through different mechanisms like virtual private networks or proxies.

However, imagine that an American writes a comment on an American blog, newspaper or social media that offers its services also in the EU and says something true about a European person. It may be going too far to force Google to de-reference it worldwide when that American was writing something

[17] Request for a preliminary ruling from the Conseild'État (France) of 21 August 2017, *Google Inc. v. Commission nationale de l'informatiqueet des libertés (CNIL)*, Case C-507/17.

[18]It is interesting to underline this takes as legal basis the Directive that preceded the GDPR.

[19] I. Falque-Pierrotin, « Pour un droit au déréférencement mondial », *Le Monde*, 29 December 2016.

 DOI: 10.17103/sybil.23.28

legal in America, in an American medium, as this will affect the freedom of expression of that person and potentially the freedom to receive information of millions of people all over the world.

Furthermore, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression of the United Nations warned that "the logic of these demands would allow censorship across borders, to the benefit of the most restrictive censors".[20] Imagine that a country as China makes all media de-reference information of the reaction to the protests in Tiananmen Square in 1989 because speaking about this is illegal in its territory. The EU should be mindful that "excessive jurisdictional claims by democratic countries undermines those countries' objections to such claims made, for example, by oppressive dictatorships."[21] In some cases, keeping walls in the application of laws to a territory may be the most respectful option with human rights.

The key question is how to balance the human rights at stake asthe result could not be the same in different states. This is the reason why the Advocate General Szpunar positioned himself on the cautious side taken in this case by Google. He considered that there could be a danger that if an authority within the EU could order de-referencing on a worldwide scale, an inevitable signal would be sent to third countries, which could also order de-referencing under their own laws. Therefore, third countries could interpret certain of their rights in such a way as to prevent persons located in a member state of the EU from having access to information they sought. The Advocate General understood that there would be a genuine risk of a race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale.[22]

Szpunar, in its Opinion, proposed the Court to declare that the search engine is not required to de-reference on all its domain names in such a way that the links at issue no longer appear, regardless of the place from which the search on the basis of the requester's name is carried out. He considered that the search engine should only be required to delete the links at issue from the results displayed following a search carried out in a place located in the EU. In that context, that operator is required to take all steps available to ensure effective and complete de-referencing. That includes, in particular, geo-blocking from an IP address deemed to be located in one of the member states regardless of the domain name used by the internet user conducting the search. In any case, the Court in its decision will have to make a very thorough balancing of rights.[23]

The Opinion in this case seems to be at odds with the one of the same Advocate General in the case *Glawischnig-Piesczek*.[24] That case, also pending a decision of the Court of Justice of the EU, refers to an

---

[20] D. Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 6 April 2018 (A/HRC/38/35), at 6.

[21] As stated by D. J. B. Svantesson, "Extraterritoriality in Data Privacy Regulation", 7(1) *Masaryk University Journal of Law and Technology* (2012), 87-96, at 92-93.

[22] Opinion of Advocate General Szpunar, 10 January 2019, Case C-507/17, *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*, § 61, ECLI:EU:C:2019:15.

[23] See B. van Alsenoy and M. Koekkoek, *The extra-territorial reach of the EU's "right to be forgotten"*, CiTiP Working Paper 20/2015, KU Leuven Centre for IT & IP Law, 2015.

[24] Opinion of Advocate General Szpunar, 4 June 2019, Case C-18/18, *Eva Glawischnig-Piesczek v. Facebook Ireland Limited*, ECLI:EU:C:2019:458.

 DOI: 10.17103/sybil.23.28

Austrian politician who sought to eliminate some comments from Facebook, as she considered them defamatory. Among other questions, the Austrian Supreme Court asked about the exceptions of liability of the Directive on electronic commerce[25] and if Facebook was supposed to retire that information worldwide or in the relevant member state. There are other dangerous questions about the need to retire also information with an equivalent meaning but this falls out of the scope of this paper.

Szpunar has being criticized, because he stated that the territorial scope of a removal obligation imposed on a host provider in the context of an injunction is not regulated by any provision of the Directive and therefore it does not preclude ordering host provider to remove worldwide information disseminated via a social network platform (§ 93).[26] In his opinion, this is a key difference with the case already explained. However, the absurd result of this differentiation will be that if something is regulated in EU Law it should in principle only be applied in the EU, but if something is regulated in national law it can be applied worldwide.[27]

A case of defamation is obviously different from a case of "right to be forgotten" and this may have had an impact on the result. Nevertheless, if we look closer to this case we may see that it is not just a case of defamation but also political speech and as the European Court of Human Rights has stated in its case-law politicians should be open to a high degree of criticism in the framework of democratic debate.[28]However, it could be difficult for the Court to consider this as it is not part of the questions posed by the national court. Therefore, the solution again is not simple as it is the case in many instances when you try to regulate content.

Szpunar adds more nuanced comments when he states that, owing to the differences between national laws and the protection of the private life and personality rights and to respect widely recognized fundamental rights, the court must adopt an approach of self-limitation. In the interest of international comity, the court should limit the extraterritorial effects of its junctions concerning harm to private life and personality rights. The implementation of a removal obligation should not go beyond what is necessary to achieve the protection of the injured person. Thus, instead of removing the content, that court might order that access to that information be disabled with the help of geo-blocking (§ 100).

The defamation example highlights some of the problems a worldwide "right to be forgotten" may face. In the United States (US), "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."[29]

---

[25] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, OJ 2000 L 178/1.

[26] See P. Cavaliere, "AG Opinion on C-18/18: Towards Private Regulation of Speech Worldwide", *European Law Blog*, published on 28 June 2019, accessed on 19 July 2019.

[27] See D. J. B. Svantesson, *Grading AG Szpunar's Opinion in Case C-18/18 – A Caution Against Worldwide Content Blocking As Default*, at 4, published on 14 June 2019, accessed on 19 July 2019 [doi: 10.2139/ssrn.3404385].

[28] See P. Cavaliere, "Facebook, defamation and free speech: a pending CJEU case", *EU Law Analysis*, published on 17 May 2019, accessed on 19 July 2019.

[29] A. Azzi, *supra* n. 11, at para. 68.

 DOI: 10.17103/sybil.23.28

(D) CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

Another field where it is possible to face a collision between the protection of personal data and other rights is the access to electronic evidence, as shown by the Court of Justice of the EU in its data retention case law.[30] This gets even more complicated when the access to data takes places across-jurisdictions. Many police investigations require information in the hands of intermediaries located in another country or hosted abroad. Therefore, it is imperative to facilitate cross-border access of police and judicial authorities to these data to enable them to prosecute crimes effectively. However, this must be done always with the necessary safeguards of human rights to ensure a fair and equitable process. Mutual legal assistance (MLA) mechanisms do not respond well to this need because they take a lot of time when the information can be sent from one jurisdiction to another with a click, and, in many cases, the information may be fragmented across jurisdictions. Response times are extremely long normally from six to 24 months and this causes that many requests and thus investigations are abandoned.[31]

This topic has been widely discussed in the EU and the US, and the latter took the legislative lead in the matter. It was pushed to do so by a case where Microsoft refused to comply with a US court warrant requesting the content of emails stored on a server in Ireland as part of a drug trafficking investigation that was taking place in the US. The case reached the Supreme Court (*United States of America v. Microsoft Corporation*)[32] and the European *Amici Curiae* on it show the EU positions in the matter.

Several members of the European Parliament involved in the drafting of the GDPR presented a brief of *Amici Curiae* in support of Microsoft. They considered that "the successful execution of the U.S. warrant would extend the scope of U.S. jurisdiction to a sizeable majority of the data held in the world's datacenters (most of which are controlled by U.S. corporations) and would thus undermine the protections of the EU data protection regime, specifically intended and designed to cover data stored in an EU Member State."[33] In this case, it is not the extraterritorial application of the GDPR that posed a

---

[30] Judgements of the Court of Justice of the EU of 8 April 2014, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General*; and *KärntnerLandesregierung, Michael Seitlinger, Christof Tschohl and others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238; and of 21 December 2016, *Tele2 Sverige AB v. Post-ochtelestyrelsen*, and *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970.

Even after the decisions of the Court, the member States continue looking for a way to create EU legislation on data retention and the Council of the EU tasked the European Commission to draft a comprehensive study on possible solutions for retaining data, in its Conclusions of 27 May 2019 (Doc. 9663/19).

[31] Cybercrime Convention Committee, *The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, 3 December 2014 (T-CY(2013)17rev), at. 123.

[32] For a good explanation of the US *Charming Betsy* canon and an in-depth study of the challenges of this case see A. J. Colangelo and A. L. Parrish, *International Law and Extraterritoriality: Brief of International and Extraterritorial Law Scholars as Amici Curiae (U.S. v. Microsoft)*,(SMU Dedman School of Law Legal Studies Research Paper No. 382, 2018), [doi: 10.2139/ssrn.3105491].

[33] *Brief of* Amici Curiae *Jan Philipp Albrecht, Sophie in 't Veld, Viviane Reding, Birgit Sippel, And Axel Voss, members of the European Parliament in support of respondent Microsoft Corporation*, at 14.

conflict with other laws, but the other way around, as the EU is not the only one following this extraterritorial trend.

The European Commission was quite cautious in its *Amicus Curiae*. It underlined that, in the EU's view, any domestic law that creates cross-border obligations should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity.[34] It also acknowledged that the application of domestic law to foreign conduct may cause friction with foreign countries and result in violations of international law, and it is necessary to mitigate such risks.[35]

The Supreme Court never decided the case, because the US Congress enacted the Clarifying Lawful Overseas Use of Data Act (H.R. 4943), known as the CLOUD Act, on 23 March 2018, rendering the case moot. This federal law states that a provider of electronic communication service or remote computing service under US jurisdiction shall preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the US. This includes personal data stored in the EU that fall under the protection of the GDPR.

The GDPR has very strict rules of when these data can be facilitated to authorities outside the EU and the simultaneous application of the GDPR and the CLOUD Act in certain cases can pose serious conflicts to Internet intermediaries, as abiding by one would mean breaching the other. The LIBE Committee of the European Parliament asked the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) about the implications of the CLOUD Act. They declared in their joint response that "unless a US CLOUD Act warrant is recognized or made enforceable on the basis of an international agreement,[36] the lawfulness of such transfers of personal data cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary to protect the vital interests of the data subject."[37]

This gets even more complicated because the European Commission has decided also to propose a mechanism to facilitate the access of European authorities to electronic evidence in criminal matters

---

34 *Brief of the European Commission on behalf of the European Union as* Amicus Curiae *in support of neither party*, at 5. Ireland did not align itself formally with Microsoft but argued that the procedures provided for in the MLA Treaty between it and the US represented the most appropriate means to address such requests and offered to process it as expeditiously as possible. *Brief for Ireland as Amicus Curiae in support of neither party*, at 11.

35 *Ibid.* at 6.

36 One of the main problems, in the opinion of the EDPB and the EDPS, is that the MLA Treaty in force between the EU and the US only aims at facilitating judicial cooperation, and therefore contains very limited provisions relevant from a data protection point of view. Another option will be the new Protocol to the Council of Europe Convention on Cybercrime to facilitate cross-border access to electronic evidence currently negotiated of which both the US and the EU are supposed to become parties when it is finalized.

37 Joint letter of the EDPB and the EDPS addressed to Juan Fernando López Aguilar, Chair of the LIBE Committee on 10 July 2019.

 DOI: 10.17103/sybil.23.28

through the creation of EU Production and Preservation Orders.[38] The draft Regulation lays down the rules under which an authority of a member state may order directly a service provider offering services in the EU, to produce or preserve electronic evidence, regardless of the location of data (Article 1.1). According to Article 2.4 of the draft, "offering services in the Union' means enabling legal or natural persons in one or more member state(s) to use the services listed in the relevant article and having a substantial connection to the member state(s)."[39] It follows although not with exactly the same wording a similar logic to the GDPR with a passive personality or target principle to justify its extraterritorial application and it will apply to a high number of companies outside the borders of the EU. This may entail further conflict with the CLOUD Act, as this has a second part which is a "blocking statute" that forbids Internet providers to facilitate data to a foreign authority if there is not an executive agreement between that state and the US. The European Commission is working to solve this problem as in May 2019 it received a mandate from the Council to open negotiations to conclude an agreement with the US on cross-border access to electronic evidence for judicial cooperation in criminal matters.

Nevertheless, this is not the only problem of the proposed Production and Preservation Orders for electronic evidence. The design of these mechanisms does not incorporate enough human rights safeguards. It places the Internet intermediaries as the only ones who could defend the interests of the data subjects as they will not be notified of the request usually. The intermediaries will not have much time to react and will not have enough information available to assess its compatibility with the human rights of the person targeted by the request so all the incentives will be to comply and none to appeal the order.[40]

(D) CONCLUSIONS

All this shows that when it comes to regulating aspects related to the Internet, in many cases, it is impossible not to resort to a certain extraterritorial effect of the rules and this may be justified in some cases. However, in others, we should consider if the use of geo-blocking is not a better solution. This

[38] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final.

[39] Recital 28 of the draft clarifies the meaning of "substantive connection" as follows "Such a substantial connection to the Union should be considered to exist where the service provider has an establishment in the Union. In the absence of such an establishment, the criterion of a substantial connection should be assessed on the basis of the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States can be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering goods or services. The targeting of activities towards a Member State could also be derived from the availability of an application ('app') in the relevant national app store, from providing local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection is also to be assumed where a service provider directs its activities towards one or more Member States as set out in Article 17(1)(c) of Regulation 1215/2012 on jurisdiction and the recognition and enforcement of judgements in civil and commercial matters."

[40] See M. Böse, *An assessment of the Commission's proposals on electronic evidence*, European Parliament, 2018 [Doi: 10.2861/247211] and *Joint Civil society letter to Member States about their draft position on "e-evidence"* of 5 December 2018.

must be analysed with special care to try to apply solutions proportional to the problems and the interests at stake.[41] It is especially important to think about what consequences any regulation will have in practice and, above all, for human rights, knowing that sometimes there will be conflicts of fundamental rights. For example, a blocking order with global scope is justified for some kinds of content as child pornography but may not be for a de-referencing order to comply with the right to be forgotten affecting freedom of expression and information in a place where such right does not even exist.

The EU is a global normative leader in Internet related laws. For this reason, its legislators should think about the consequences of the extraterritorial application of its laws because certain countries that do not share its democratic values could do with similar laws if they applied them for spurious reasons. Although the Internet by its very nature knows no limits, the regulation of many of the aspects linked to it must do so. However, this should not stop us when considering norms that may increase the standard of the protection of human rights worldwide as the GDPR.

The cross-border access to electronic evidence would be better regulated by international treaties, where that is possible, than by unilateral measures. The way forward is to negotiate an agreement between the EU and the US and a Protocol to the Cybercrime Convention that contain the necessary human rights safeguards.

The EU must ease access to electronic evidence in criminal matters but the proposed production and preservation orders have to include also the appropriate human rights safeguards. This mechanism may be mimicked in others parts of the world so the EU should be coherent with its aim of increase the respect for human rights globally. Both the CLOUD Act and the European Commission proposal should be amended to improve their mechanisms to solve conflicts of laws as they would surely appear sooner than later.

Another issue common to the right to be forgotten and the production and preservation orders and many other initiatives related with online regulation is that we place Internet intermediaries as the ones who will have to decide in "the first instance" if they reject or grant these requests (not the person who created the content or the data subject). In most cases, they would be businesses moved by the increase of their benefits not by the well-being of their users so we have to make sure not to privatize law-enforcement and not to create incentives heavily weighted on the side of ignoring the rights of users and just comply with any request they get. States cannot relinquish their primary responsibility to protect human rights in the name of efficiency and swiftness. This may also mean the need to create new avenues of accountability for Internet intermediaries.[42]

The question at the end it is not really if we should build walls or break them but how to create laws that may go beyond borders or stop at them as the best solution in each case. In this sense, as in many others, the reply should be to do whatever improves the protection of human rights taking the necessary measures that follow legitimate goals in a proportional way.

---

[41] See J. C. Daskal, "Speech Across Borders" (February 21, 2019). *Virginia Law Review* (2019), [doi.org/10.2139/ssrn.3407716].

[42] Kaye, *supra* n. 20, at 20.

 DOI: 10.17103/sybil.23.28

DOI: 10.17103/sybil.23.28