Challenges to the extraterritorial enforcement of data privacy law – EU case study

Michal Czerniawski and Dan Svantesson*

1. Introduction

States implementing data privacy laws must carefully consider how they delineate the scope of application of those laws. The 'extraterritorial' application of a country's data privacy laws may severely impact different actors outside its borders including e.g., their freedom of expression and their financial interests. At the same time, it is clear that, to ensure effective protection of data subjects' rights, modern data privacy laws must have extraterritorial application. Different attitudes towards privacy and data protection globally and the lack of global standards fuelled a heated debate among those emphasizing the need for jurisdictional restraint and those stressing the need to ensure effective protection. In the light of this, the way in which a data privacy law's extraterritorial application is delineated requires a careful balancing of important interests. In the European Union's General Data Protection Regulation ('GDPR'), it is Article 3 that performs this function, and in this chapter, we make some observations about how well Article 3 works in this role. However, before doing so, we first examine the role that 'extraterritoriality' plays in data privacy law and discuss how the "hero" of this volume – Datalagen (1973:289) (hereinafter 'Datalagen') – and its evolution in Swedish law, related to extraterritoriality.

Moreover, in this paper we discuss the topic of extraterritorial enforcement of EU laws. Lack of sufficient enforcement questions the legitimacy of the state's claims and ultimately – its governance.[1] We believe that the problems with extraterritorial enforcement may at

* An EU official, the views and opinions expressed in this paper are those of the authors and do not necessarily reflect the views or positions of any entities, particularly the European Parliament.

[1] Ch. Reed, Cloud Governance: The Way Forward, [in:] Christopher Millard (ed.), Cloud Computing Law, Oxford 2013, p. 363.

some point become one of the burning problems of the European Union in its attempts to regulate the digital environment. Finally, we briefly suggest blacklisting as one of the tools that could be used by the EU to facilitate the effective enforcement not only of the GDPR, but also of other laws with extraterritorial effect.

2. The role that 'extraterritoriality' plays in data privacy law

A key conundrum we are faced with can be expressed as follows: extraterritorial jurisdictional claims are reasonable because if states do not extend their data protection to the conduct of foreign parties, they fail to provide effective protection for their citizens' rights. At the same time, wide extraterritorial jurisdictional claims are arguably unreasonable because it is not possible for those active on the Internet to adjust their conduct to all the laws of all the countries in the world with which they come into contact. In other words, a widespread extraterritorial application of state law may well end up making it impossible for businesses to engage in cross-border trade.

Bearing in mind the central role played by the concept of extraterritoriality in this chapter, it is prudent to discuss the exact meaning of that concept. Put simply, jurisdictional claims are typically said to be either territorial or extraterritorial, with the latter type generally defined as relating to the exercise of jurisdiction by a state over activities occurring outside its borders. Modern communications technology, however, undermines such a binary division. For example, is a state exercising jurisdiction over activities occurring outside its borders where it regulates the use of personal information about its citizens stored in a cloud computing arrangement with multi-jurisdictional reach?

The binary distinction between territorial and extraterritorial is one of the most central concepts under stress in the online environment. Like other binary simplifications, such as the distinction between day and night, and between ales and lagers, it works for certain purposes, but it is inadequate for other important purposes. Much like the failure of the day/night distinction to consider dusk and dawn, and indeed the many nuances in between, viewing the strength of jurisdictional claims from the binary perspective of territorial versus extraterritorial does not adequately reflect the nuances involved.

Further, even if we were able to draw a sharp line between jurisdictional claims that are territorial and those that are extraterritorial, identifying a jurisdictional claim as being extraterritorial tells us little,

or nothing, of value. Some extraterritorial claims can be indisputably legitimate and useful (after all, they may be based, e.g., on the widely recognized nationality principle), while other extraterritorial claims are equally indisputably illegitimate and excessive.[2] Yet too often – especially in the Internet context – the ill-advised territorial/extraterritorial distinction is used as shorthand for legitimate (i.e., territorial) claims versus illegitimate (i.e., extraterritorial) claims of jurisdiction.[3] Such oversimplifications are misguided and unhelpful and invariably create obstacles for a fruitful debate.

The best we can expect to achieve when it comes to the concept of extraterritoriality is to bring some clarity and consistency as to what we discuss as being 'extraterritorial'. Extraterritoriality may relate to at least the following:

1. conduct that is being regulated may be, wholly or partly, initiated extraterritorially;
2. conduct that is being regulated may be, wholly or partly, completed extraterritorially;
3. conduct that is being regulated may have, wholly or partly, extraterritorial effects; and
4. extraterritorial objects, including things and legal or natural persons, may be the direct or indirect objects of regulation.[4]

All four of these categories may be of relevance in the context of the claims of jurisdiction made in data privacy laws, and it is clearly challenging to devise jurisdictional criteria that capture situations to which the law should apply without also capturing situation to which it would be excessive and unjustified to apply the law. This is a serious issue in relation to which there are no easy solutions.

Modern data privacy laws are complex instruments that seek to achieve a wide range of objectives. Thus, the idea of having one single jurisdictional threshold for the entire law, such as in the GDPR, might be seen as questionable and risks undermining the legitimacy of such laws. Moving forward the drafters of data privacy laws ought to con-

[2] See further: D.J.B. Svantesson, 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5 International Data Privacy Law 226; and Ch. Kuner, 'Extraterritoriality and International Data Transfers in EU Data Protection Law' (2015) 5 International Data Privacy Law 235. Ch. Kuner, Data and extraterritoriality, [in:] A. Parrish & C. Ryngaert (ed.), Research Handbook on Extraterritoriality in International Law, Cheltenhamp/Northampton 2023.

[3] For an example of such a point of view, see Joanne Scott, 'The New EU "Extraterritoriality"' (2014) 51 Common Market Law Review 1343, 1345.

[4] See further: D.J.B. Svantesson, *Private International Law and the Internet 4th Ed.* (Kluwer Law International, 2021), at 13–15.

sider adopting what has been referred to as a 'layered approach' in which the relevant substantive law (here the various substantive provisions of a data privacy law) is divided into different layers, with a different jurisdictional threshold for the various layers.[5] For example, it may have been fruitful to assign provisions such as Article 6 GDPR to an "abuse-prevention layer" in relation to which a far-reaching claim of jurisdiction may be justified. In contrast, provisions such as Article 37 GDPR could fall within an "administrative layer" in relation to which the jurisdictional threshold would be high. And provisions such as Article 15 GDPR (giving a right of access by the data subject) could fall within a "rights layer" in relation to which the jurisdictional threshold would be easier to satisfy that for the administrative layer, but more difficult to satisfy that for the abuse prevention layer.[6]

To illustrate the practical implications of the layered approach, imagine that an e-commerce business in Australia is predominantly active on the Australian market, but that it is also has a small number of customers in Thailand and in the EU. Under the current legal landscape, that business would need to comply with the full data privacy laws of Australia, Thailand and the EU perhaps including highly burdensome provisions such as Article 37 GDPR requiring the business to designate a data protection officer. Had the data privacy laws of Australia, Thailand and the EU adopted the layered approach, the outcome would have been different. Clearly the Australian business – given its substantial presence on the Australian market – would be required to comply with the full (all layers of) Australian data privacy law. However, with its very limited interaction with the EU and Thai markets, the business would likely only need to consider those rules of Thai and EU data privacy laws falling into the "abuse-prevention layer". And given that those provisions are generally the same across most data privacy laws in the world, the added compliance burden would be negligible compared to under our current structure.

This 'layered approach' recognises that the multifaceted nature of modern data privacy law necessitates a departure from one size fits all

[5] D.J.B. Svantesson, A "layered approach" to the extraterritoriality of data privacy laws, *International Data Privacy Law*, Volume 3, Issue 4, November 2013, Pages 278–286, https://doi.org/10.1093/idpl/ipt027.

[6] The only aspect of the GDPR in relation to which it may be said that there is a jurisdictional threshold derogating from that of Article 3 is in Article 27 – a provision we discuss in some detail below. There it is made clear that the obligation prescribed under Article 27 – that of controller and processors caught by Article 3(2) having an obligation to designate in writing a representative in the Union – does not apply to: "processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing;".

style delineations of extraterritoriality in favour of a more nuanced and sophisticated approach befitting environments of multiple overlapping applicable laws. It responds to the need to balance important interest and would give early adopters the world's most modern and sophisticated approach to delineating the territorial scope of application of a data privacy law.

Obviously, it is also an arrangement that benefits international cooperation since, the more states adopt a layered approach, the easier will it be to ensure the protection of data subjects' privacy while still creating an environment friendly to cross-border business. Put simply, the 'layered approach' is a structure aimed at creating a level playing field on an international level, not just within the EU market. But we are not there (yet), and a detailed discussion of how we may geta widespread adoption of this more modern 'layered approach' goes beyond the scope of this paper.

3. The territorial scope of the Datalagen

As many of the other contributions to this volume makes clear, reading the groundbreaking Datalagen now – some 50 years later – is doubtlessly an enriching experience. One may, for example, be struck by how much is covered in the 25 Articles – over five and a half pages – that make up the law. Frankly, the impressive brevity of the Datalagen may legitimately make us question whether the GDPR really needs to be 99 Articles taking up some 88 pages.

At the same time, it is striking how different is the world that the Datalagen sought to tame compared to the world that the GDPR seeks to regulate. Provisions such as Datalagen's Article 22 stand out. Under the Article, violations of Datalagen may result in the data being forfeited. Without necessarily condoning the 'race to the highest fines' that we are seeing in today's data privacy laws, those bemoaning the high fines that may be awarded under modern data privacy laws may wish to stop and ponder how a provision like Datalagen Article 22 would impact the data-driven businesses of today.

While Datalagen contained a restriction on transborder data flows,[7] it did not contain any provision giving the law any extraterritorial scope of application. Indeed, the fact that the Datalagen is territorially lim-

[7] Art. 11. See further: D.J.B. Svantesson, A legal method for solving issues of Internet regulation; applied to the regulation of cross-border privacy issues, European University Institute Working Paper LAW2010/18, https://cadmus.eui.eu/bitstream/handle/1814/15344/LAW_2010_18.pdf?sequence=1&isAllowed=y.

ited to Sweden can be said to be implied in many of its provisions. For example, the Datalagen authorises the data protection authority of the time ('Datainspektionen') to access the physical facilities at which the data processing takes place.[8] It is difficult to imagine such a provision having an extraterritorial scope of application.

While the absence of claims of extraterritorial application may be surprising by reference to modern data privacy laws, Datalagen must obviously be read in its context. In particular, it is clearly a law aimed at addressing the complexities faced in a world predating widespread Internet use. As noted by Kuner:

> "When one examines academic writings, case law, and legislation relating to international jurisdiction, it becomes clear that, prior to the internet, there never existed a situation in which a state purported to extend the application of its law to many millions of entities in different countries around the world based on the fact that they were accessible by, or processed data of, citizens of the home jurisdiction."[9]

Having said that, this should not be seen to imply that the issues of extraterritoriality were not on the mind of the lawmakers of the time. For example, the authors of SOU 1993:10 discuss how to address a situation where the content of Swedish newspapers are transferred to CD-ROM abroad, and then marked in Sweden.[10]

Despite its many amendments, Datalagen never included any provision giving it extraterritorial scope. The Swedish position only changed through the introduction of the Personuppgiftslagen in 1998.

4. The territorial scope of the Personuppgiftslagen

As a result of the EU membership, the Swedish data privacy law was reformed leading to the adoption of the Personuppgiftslag (1998:204). Being based on the EU's Data Protection Directive it incorporated Article 4 of that Directive:

[8] Article 16.

[9] Christopher Kuner, European Data Protection Law: Corporate Compliance and Regulation 2nd Ed. (Oxford University Press, 2007, Oxford), at 123–124.

[10] "Ett annat problem med att låta datalagen vara tillämplig har med den tekniska utveckligen att göra. När det gäller utländska tidskrifter finns det redan i dag hela årgångar på CD-ROM-skivor. Kostnaderna för att föra över informationen på CD-ROM-skivor kan förväntas sjunka kraftigt i framtiden. Frågan är då hur man skall hantera det problemet att man utomlands låter överföra äldre årgångar av svenska tidningar på CD-ROM-skivor, som därefter saluförs i Sverige." (SOU 1993:10, at 147).

> 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: [...]
>
> (a) the processing is carried out in the context of *the activities of an establishment of the controller on the territory of the Member State*; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
>
> (b) the controller is not established on the Member State's territory, but in a place where its *national law applies by virtue of international public law*;
>
> (c) the controller is not established on Community territory and, for purposes of processing personal data *makes use of equipment, automated or otherwise, situated on the territory* of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community. (emphasis added)[11]

As pointed out by the European Commission in relation to the 1992 Amended Proposal for the Directive, the intention of Article 4 is to avoid two possibilities: (1) "that the data subject might find himself outside any system of protection, and particularly that the law might be circumvented in order to achieve this"[12] and (2) "that the same processing operation might be governed by the laws of more than one country".[13]

At any rate, with this development, Swedish data privacy law finally incorporated an express articulation of the law's extraterritorial scope of application. However, interestingly the most famous 'extraterritorial' application of the Personupgiftslagen – that of the action against Google Inc in relation to the so-called "right to be forgotten" – nevertheless relied on Article 4(1)(a); that is, the activities of an establishment of the controller on the territory of the Member State.[14]

It may here be noted that the EU Directive's approach to data privacy (and therefore the approach taken in Personuppgiftslagen)– including its extraterritorial scope – has been subject to criticism. For example,

[11] Personuppgiftslag (1998:204), Art. 4.

[12] COM (92) 422 final – SYN 287, 15 October 1992, 13. Recital 20 in the preamble to the Directive gives some additional guidance as to this goal:

> Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice.

[13] For a more detailed analysis of the Directive's territorial scope, see M. Czerniawski, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in D.J.B. Svantesson and D. Kloza (eds), Transatlantic data privacy as a challenge for democracy (Intersentia 2017).

[14] https://www.imy.se/globalassets/dokument/beslut/2017-05-04-google.pdf.

one commentator has argued that ECJ cases have shown that "the rights extended to E.U. citizens by the [Data Protection] Directive fail to recognize the practical realities of how data is used in global commerce".[15] Indeed, another commentator concluded that the very establishment of a data privacy standard of the kind found in the EU Directive offends the sovereignty of non-EU countries:

> "Regardless of the European Union's motivations, there is no denying that the effect of the Directive transcends sovereign borders. By unilaterally establishing the standard for protection, the E.U. has unquestionably 'intervene[d] in the internal or external affairs of' third countries. These sovereign states must either comply with the will of a foreign power, or be effectively sanctioned via a blacklist."[16] (footnotes omitted)

This reasoning lacks sting as it would mean that many aspects of a country's substantive law infringe on the sovereignty of other states.[17] For example, a ban on certain food additives in state A would violate the sovereignty of all states that do not have a ban on such food additives since manufacturers in those states are prevented from selling their products in state A – state A is intervening in the internal or external affairs of third countries since these sovereign states must either comply with the will of a foreign power (i.e. change their law so as to also ban the said food additives), or be effectively sanctioned via a blacklist from having their manufacturers sell the goods in question to state A.

Indeed, the principles underlying this notion to treat foreign actors on a market equally to domestic actors on that market, by extending personal jurisdiction over those foreigners, has a long history. For example, in his classic *On the Law of War and Peace*, Hugo de Groot (better known as Hugo Grotius) wrote that: "for the government of a people, it is morally necessary that foreigners who mingle with them even temporarily – as happens when foreigners enter a country – should conform

[15] Edward C Harris, 'Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answers' (2006–2007) 22 American University International Law Review 746, 798.
[16] Joshua S. Bauchner, State sovereignty and the globalizing effects of the Internet: A case study of the privacy debate 26 Brook. J. Int'l L. 689 2000–2001, at 715.
[17] It needs to be acknowledged that an argument similar to that presented by Bauchner could be advanced in reliance on international trade agreement obligations, such as under the World Trade Organization's General Agreement on Trade in Services. However, that is a separate issue falling outside our scope here. For an insightful discussion of the EU Directive's status in relation to GATS, see e.g.: Carla L. Reyes, WTO-complaint protection of fundamental rights: Lessons from the EU Privacy Directive, *Melbourne Journal of International Law* Vol 12 (2011).

to the institutions of that people."[18] This principle is no less important today than it was in the 1600s when it was expressed by Grotius.

Unsurprisingly, when the EU proceeded with the modernisation of its data privacy law – in the form of the GDPR bringing the end of the Personuppgiftslagen – the practice of making an extraterritorial claim of application continued.

5. Five years of the extraterritorial reach of the GDPR

Earlier this year, on 25 May 2023, we were celebrating five years since the GDPR became applicable. It is therefore a good moment to pause and consider the impact of the GDPR. Here we will examine what the application of the GDPR outside the EU borders looks like in practice.

During these five years, we have witnessed some positive developments in particular linked to the so-called "Brussels effect"[19] and the indirect impact that the GDPR has had globally, but we also note some developments that could be worrying; not only in the context of the GDPR, but also in the context of other EU laws. At this stage of the paper, we will discuss two cases that we believe clearly illustrate problems with the extraterritorial enforcement of the GDPR. They cover processing of personal data by third-country controllers or processors that fall under the scope of Article 3(2) of the GDPR but who are not willing to cooperate with European data protection authorities. The first one deals with enforcing decisions of the national data protection authorities outside of the European Union in situations where a data controller or a processor does not recognise EU jurisdiction, and the second with a failure to designate a representative.

It would be difficult to disagree with Greenleaf that "[d]ata privacy laws on paper mean little by themselves, even if they are ubiquitous. It is only through evidence of their enforcement, or through convincing evidence of compliance with them irrespective of enforcement, that we can be satisfied that they cause behavioural change."[20] As Reed points out 'the enforcement power of states is far lower in cyberspace than in the physical world'.[21] In this context, special attention should be given

[18] Stephen C. Neff Ed., *Hugo Grotius On the Law of War and Peace* (2012, Cambridge University Press, Cambridge), at 96.
[19] A. Bradford, The Brussels Effect: How the European Union Rules the World (New York, 2020; online edn, Oxford Academic, 19 Dec. 2019), accessed 19 July 2023.
[20] G. Greenleaf, Global Data Privacy Laws: EU Leads US and the Rest of the World in Enforcement by Penalties (February 4, 2023). (2023) 181 Privacy Laws & Business International Report 24–29.
[21] Ch. Reed, Cloud Governance: The Way Forward, [in:] Christopher Millard (ed.), Cloud Computing Law, Oxford 2013, p. 363.

to Article 3(2) GDPR, the so-called "long arm" of the Regulation and the topic of extraterritoriality.

Problems with enforcement of the GDPR outside its borders may have consequences for the legitimacy of the EU. Therefore, the effective extraterritorial enforcement of the GDPR is arguably crucial for the credibility of the EU as an actor on the global stage.

Before concluding this part, we note in passing that the problems with the enforcement of the GDPR are not strictly limited to situations involving extraterritorial enforcement. We notice worrying issues also with the GDPR enforcement within the EU territory. The number of cases resolved via the one-stop-shop mechanism is still not satisfactory and the decision-making process is very lengthy. Moreover, we lack answers to some key questions about the enforcement e.g., how many of the decisions issued by DPAs in the last five years were invalidated by the courts or how many GDPR fines were actually paid. For example, the two highest fines imposed by the Polish DPA, which made headlines both in Polish and European media, were both subsequently invalidated by the administrative courts.[22] These matters clearly deserve further attention. However, they lie outside the scope of this chapter and will not be discussed further here.

5.1 A brief summary of Article 3(2) GDPR

The EU data protection regime is the most influential and one of the strictest data privacy laws in the world.[23] Although already the GDPR predecessor, Directive 95/46/EC,[24] (as noted above) included provisions on extraterritorial scope, a real change came with the GDPR.[25]

[22] The amount of fines was respectively: 2,8 million PLN (currently around 0,6 million EUR) on Morele.net and 4,9 million PLN (currently around 1,1 million EUR) on Fortum Marketing and Sales Polska. See S. Wikariak, Rekordowa kara 5 mln zł uchylona przez sąd, Dziennik Gazeta Prawna, published on 8 May 2023.

[23] See among others, D.J.B. Svantesson, *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing, Copenhagen 2013, pp. 21 and 89; L.A. Bygrave, 'Privacy and Data Protection in an International Perspective' (2010) 56 *Scandinavian Studies in Law*, 183; M. Taylor, 'The EU's human rights obligations in relation to its data protection laws with extraterritorial effect' (2015) 5 *International Data Privacy Law*, 246.

[24] Directive (EC) 95/46 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.

[25] Drafters of the directive worked on it in the early 90 of the last century, in a totally different technological reality, and could not have a global perspective on the territorial scope of law which we have today. Moreover, drafting a directive and not a regulation, it seems they were focusing on regulating data flows within, and not outside, the EU. See M. Czerniawski, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in D.J.B. Svantesson and D. Kloza (eds), Transatlantic data privacy as a challenge for democracy (Intersentia 2017).

The GDPR's extraterritorial scope based on a moderate destination approach[26] played an important role in what Kuner called a Copernican revolution in EU data protection law.[27]

Article 3(2) GDPR outlines what types of interaction with the EU will activate the application of the GDPR, in this sense GDPR territorial scope is not "classically" extraterritorial, as it largely focuses on regulating activities conducted by third-country entities that take place in the EU. The GDPR's territorial scope is partly territoriality-dependent and partly territoriality-independent.[28] It was design to ensure, or at least justified by reference to the aim of ensuring, a 'level playing-field' between businesses based in the EU and the non- EU based businesses operating on the European market. It is also driven by the reasoning applied by the CJEU in cases such as C-131/12 *Google Spain* and C-230/14 *Weltimmo* that fundamental rights need to be effective.[29] In the digital age, this requires enforcing data protection rights also against non-EU entities.

The main extraterritorial scope of the GDPR is introduced in its Article 3(2), which regulates situations when a controller or a processor is not established in the EU and a data subject is physically present in the Union. Article 3(2) GDPR requires that one of the two criteria, both based on "targeting" and market access trigger, is met: processing activities are related to the offering of goods or services to data subjects in the Union or to the monitoring of their behaviour, as far as their behaviour takes place within the Union. Both criteria require a degree of "intention to target" on the part of the data controller or processor.

Under the GDPR, processing activities must be *related to* either offering of goods or services to data subjects in the EU, or to the monitoring of their behaviour. Reference to 'related to' requires a connection between the processing activities on the one hand and the offering

[26] The approach 'which only gives targeted States the right to regulate the activity' is called by Kohl a 'moderate destination approach'. See U. Kohl, 'Jurisdiction in cyberspace', [in:] N. Tsagourias and R. Buchan (ed.), Research Handbook on International Law and Cyberspace, p. 35. For a comprehensive analysis of the targeting criterion see B. van Alsenoy Reconciling the (extra)territorial reach of the GDPR with public international law, [in:] G. Vermeulen, E. Lievens (eds), Data Protection and Privacy under Pressure. Transatlantic tensions, EU surveillance, and big data 2018.

[27] The term "Copernican revolution" in the context of the EU data protection reform was first used by Ch. Kuner, '*The European Commission's Proposed Data Protection Regulation:* A *Copernican Revolution in European Data Protection Law*', Bloomberg BNA Privacy and Security Law Report, 6 February 2012, pp. 1–15.

[28] D.J.B. Svantesson, 'Article 3 Territorial scope', in Ch. Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, 2020; online edn, Oxford Academic), accessed 8 July 2023.

[29] P. de Hert, M. 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*, Volume 6, Issue 3, August 2016, pp. 230–243.

of goods or services or monitoring of the behaviour on the other. The European Data Protection Board (hereinafter: EDPB) stated that "Article 3 of the GDPR reflects the legislator's intention to ensure comprehensive protection of the rights of data subjects in the EU and to establish, in terms of data protection requirement, a level playing field for companies active on the EU markets, in a context of worldwide data flows".[30]

5.2 Brussels Effect – the success story of the GDPR

We begin this section with the area where the GDPR succeeded the most. Bradford describes the "Brussels Effect" as European Union's "unilateral ability to regulate global markets by setting the standards in competition policy, environmental protection, food safety, the protection of privacy, or the regulation of hate speech in social media".[31] She draws a distinction between *de facto* Brussels Effect and *de jure* Brussels Effect,[32] the first understood as compliance with EU legislation by companies, the latter meaning third countries adopting EU-style legislation. As regards *de facto* Brussels Effect it should be underlined that it is achieved via a voluntary compliance with the GDPR requirements by non-EU companies that operate globally. The companies complying with the GDPR have a strong incentive to do that: the EU is a big multinational market with almost 450 million consumers, and those who want to offer their goods or services on the European single market, need to comply with its requirements. Bradford leaves no doubt that the compliance is directly linked to the EU's market power and the fact that the EU consists of some of the wealthiest states in the world: "the EU is one of the largest and wealthiest consumer markets, supported by strong regulatory institutions. There are few global companies that can afford not to trade in the EU".[33] What seems to make a difference and makes the compliance effort worth it, is that by complying with a single set of rules, companies can operate in 27 European countries.

Furthermore, the *de jure* Brussels Effect of the GDPR seems to be proven by data. The most recent information gathered by Greenleaf shows that there are 162 countries with data privacy laws[34], an increase

[30] European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version 2.1, 7 January 2020, p. 4.
[31] A. Bradford, The European Union in a globalised world: the "Brussels effect", https://geopolitique.eu/en/articles/the-european-union-in-a-globalised-world-the-brussels-effect/, last access: 22.07.2023.
[32] Ibid.
[33] Ibid.
[34] G. Greenleaf, Global Data Privacy Laws 2023: 162 National Laws and 20 Bills (February 10, 2023). (2023) 181 Privacy Laws and Business International Report (PLBIR) 1, 2–4.

by 42 countries since 2017,[35] i.e., one year before the GDPR became applicable. Many of these laws are inspired by, or indeed largely imitations of, the EU legislation.

The global influence of the EU in the privacy and personal data protection area seems to be amplified by the (current) lack of federal data privacy laws in the United States of America and by the fact that the other regulatory superpower – China – fails to respect human rights and fails to maintain a predictable and transparent regulatory environment. This results in a situation where there is no other similar standard that could be considered as competitive to the EU approach on the global arena, although regional guidelines and instruments can be found in various parts of the world.

We firmly believe that what makes the EU laws, including the GDPR, so appealing, besides the market aspect, is the values protected by the European Union. The EU is known for its respect for human rights – it created, and with Court of Justice of the European Union rulings constantly develops – the concept of fundamental rights. Those third countries that take inspiration from EU regulations, also benefit from its experience and expertise in fundamental rights. The value-based philosophy differs from the US approach that largely relies on the market as the main regulating power and from the Chinese approach which puts the needs of the ruling Communist party in the first place. Additionally, it allows companies to create an image of a business that takes care of consumers and their rights and comply with the highest possible standards. Bradford summarises this landscape as follows: "US techno-libertarianism is now widely held to be obsolete, while the Chinese digital authoritarianism is inacceptable; therefore, the best way to gain [...] consumers' trust might be to subscribe to EU rules and underlying values, which are generally well thought and produced through an appropriate legislative process".[36] These factors, and not "hard" law or the risks of possible sanctions, push third country as well as controllers and processors established in third countries into complying with the GDPR norms.

Finally, the incentives are also generated by EU-established companies that impose GDPR standards on their non-EU contractors and sub-contractors, thus contributing to the even broader spreading of

[35] G. Greenleaf, Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey (January 30, 2017). (2017) 145 Privacy Laws & Business International Report, 10–13, UNSW Law Research Paper No. 17-45.

[36] A. Bradford, The European Union in a globalised world: the "Brussels effect", https://geopolitique.eu/en/articles/the-european-union-in-a-globalised-world-the-brussels-effect/, last access: 22.07.2023.

the European standards globally. All these mechanisms can be seen as a part of the European Union's digital expansionism.

5.3 The struggle of enforcing GDPR against Clearview AI

A five-year period of application is an insufficient basis on which to draw extensive and definitive conclusions. However, one of the signs that the GDPR's extraterritorial enforcement may require some additional tools might be found in the Clearview AI cases.

Clearview AI is a facial recognition platform designed to support federal, state, and local law enforcement. It is a US-based company, without establishments in the European Union. The European Data Protection Supervisor provided the following description of the company: "Clearview AI is an American private company offering a browser-based product through which users can upload facial images for analysis and cross-checking against a database of images scraped by Clearview from a variety of sources, including social media."[37] According to information from Clearview AI's website, they store more than 30 billion images of individuals.[38]

Four EU data protection authorities issued decisions against Clearview AI concluding that the company breached the GDPR by conducting facial recognition on public web sources and prohibited further processing. These were:

1) Garante (Italy), in its decision of 10 February 2022, in which it fined Clearview AI €20M;
2) Hellenic DPA (Greece) in its decision of 13 July 2022, in which it fined Clearview AI €20M;
3) CNIL (France), in its decision of 17 October 2022, fined Clearview AI Inc €20M;
4) Austrian DPA in its decision of 10 May 2023 found Clearview AI Inc infringing Articles 5, 6, 9, 27 GDPR and the company was ordered to erase the complainant's personal data and to designate a representative within the European Union, however, did not impose any fine.[39]

[37] See EDPS Opinion on the possibility to use Clearview AI and similar services at Europol (Case 2020-0372).
[38] https://www.clearview.ai/, last access: 23.07.2023.
[39] https://edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en, last access: 23.07.2023. It may also be noted that, at the time of writing, the Swedish Integritetsskyddsmyndigheten is pursuing a matter against the Polismyndigheten's use of Clearview AI (see further: https://www.imy.se/tillsyner/polismyndigheten/).

The last decision, issued by the Austrian DPA earlier this year deserves special attention: contrary to the other data protection authorities, the Austrian DPA did not impose a fine on Clearview AI. The motives behind this decision, which goes against the approach adopted by the three other authorities, remain unclear, however one of the possible reasons might be awareness of the authority that they will not be able to enforce any administrative fine against the company. The Austrian authority limited itself to ordering Clearview AI to appoint a representative in the EU. This order seems to have been ignored, as at the time of this paper's completion, Clearview AI has no representative in the EU. The reason for that might be that the company continuous to not recognise the jurisdiction of the EU data protection authorities.

Indeed, in the context of the French decision, Clearview AI directly stated that it does not recognize the European authorities' jurisdiction.[40] In the case of the GDPR and data protection laws, extraterritorial enforcement is left to the Member States, so now we have to wait to see whether, and if so – how, respectively, France, Italy, Greece and Austria will be trying to enforce the decisions of their authorities. It seems that they have no choice but to find a way to do that, as the rules of Article 3(2) GDPR are mandatory and not only any attempt to change them (for example, by choosing different rules on jurisdiction or making choice of law in an online privacy policy or in a contract) is null and void, but also they oblige Member States to seek effective enforcement. Lack of enforcement actions by Member States could ultimately lead to infringement proceedings under Article 258 TFEU.[41] In any case, we may expect that this process may take years and there is no guarantee that Member States and their data protection authorities will be successful. The Clearview AI denial is a good example of how difficult it can be to enforce the provisions of the GDPR outside of the EU territory, not only against controllers and processors from the US, but also, for example, China, India, Russia, etc. in the case of their lack of willingness to cooperate or rejection to recognize EU's jurisdiction.

[40] Clearview denies jurisdiction of French regulator in response to €20M fine, https://www.biometricupdate.com/202210/clearview-denies-jurisdiction-of-french-regulator-in-response-to-e20m-fine, access: 23.07.2023.

[41] According to this Article "If the Commission considers that a Member State has failed to fulfil an obligation under the Treaties, it shall deliver a reasoned opinion on the matter after giving the State concerned the opportunity to submit its observations. If the State concerned does not comply with the opinion within the period laid down by the Commission, the latter may bring the matter before the Court of Justice of the European Union.". See Consolidated version of the Treaty on the Functioning of the European Union, Official Journal 115, 09/05/2008 P. 0160 – 0160.

5.4 Problems with the extraterritorial enforcement and their impact on DSA and AI Act

In 2021, European Data Protection Board commissioned a study on the extraterritorial enforcement of the GDPR.[42] This study, which went rather unnoticed, may give us reasons to worry about the extraterritorial enforcement of the GDPR, but also of other EU laws, as some new EU legislation – including the AI Act[43] and the DSA[44] – base their jurisdiction on the GDPR.

The study was commissioned by the EDPB, and not prepared by the Board. Nevertheless, it heavily relies on feedback received from EDPB Members, which are national data protection authorities. The authors of the study reach rather grim conclusions, such as that:

> "there are uncertainties as to the possibility for SAs to initiate legal proceedings in another EU Member States or in a third country on the basis of Article 58(5) of the GDPR. The Court of Justice of the European Union (CJEU) case-law is unclear as to whether it could accept to recognise the jurisdiction of a Member State on the basis of Article 58(5) of the GDPR when the controller/processor has no establishment on the territory of any EU Member State."[45]

The authors of the study point out that European data protection authorities in theory could exercise their investigative and corrective powers "in a manner that produces effects beyond the EEA territories" within the framework of the relevant international law.[46] However, there is no guarantee that third countries will recognise data protection authorities' jurisdiction. There is also a number of other doubts, such as whether European data protection authorities are even allowed to send agents abroad to third countries, even with the consent of the controllers/processors established in those countries.[47]

The authors of the study also conclude that strengthening of international cooperation seems to be the best way forward for better enforcement against third-country controllers or processors that fall under the

[42] Study on the enforcement of GDPR obligations against entities established outside the EEA but falling under Article 3(2) GDPR. Final report.
[43] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final.
[44] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
[45] Study on the enforcement of GDPR obligations against entities established outside the EEA but falling under Article 3(2) GDPR. Final report, p. 5.
[46] Ibid., p. 20.
[47] Ibid., p. 6.

scope of Article 3(2) of the GDPR but that are not willing to cooperate with SAs and did not designate an EEA representative.[48] In the short term, they suggest the adoption of Memorandums of Understanding (hereinafter: MoU) or equivalent agreements. For serious breaches of the GDPR that amounts to a criminal offence, they see the possibility to rely on Mutual Legal Assistance Treaties (MLATs). Finally, they suggest adding relevant provisions on enforcement, by the European Commission when negotiating trade agreements.[49]

These solutions do not sound very convincing for us. Let us just note that in vast majority of the Member States, GDPR breaches are breaches of the administrative law and subject to administrative and not criminal sanctions. Furthermore, third country data protection authorities cannot simply apply EU laws; thus, MoUs will not necessarily help with the enforcement of decisions issued in the EU. As regards cooperation between EU and non-EU data protection authorities in line with Article 50 GDPR, although such a cooperation can facilitate investigations and sharing of information, it will not help with extraterritorial enforcement as data protection authorities are not competent to enforce each other's decisions. Each data protection authority benefits from decision-making autonomy, they also apply respective national laws which for example regulate procedures. Finally, the cooperation mentioned in Art. 50 GDPR is voluntary.

In the EDPB study, several data protection authorities, such as those of Slovenia, Luxemburg and Iceland clearly indicated that they do not have the power to summon a non-EU controller or processor to appear before them. In some other cases the answers indirectly indicate that there might be no such possibility.

The EDPB study describes other situations where DPAs were not able to enforce the GDPR against non-EU controllers or processors:[50]

1) a case where the French authority could not clearly identify the controller of a website, but the processor was identified as a Moroccan company, after learning from the Moroccan DPA that the controller was a company in Brazil, the CNIL chose not to continue the investigation as it would not have been able to enforce corrective powers on a Brazilian company;
2) a case where the French authority investigated a major data breach concerning French data subjects. When the non-EU controller failed to reply to initial questions, the CNIL sent a letter to remind it of

[48] Ibid, p. 6.
[49] Ibid, p. 6–7.
[50] Ibid, p. 34–35.

its legal obligations. The CNIL admitted that they were not able to enforce their corrective powers in this case;

3) a case where the Lithuanian authority sent questions to a non-EU controller, but no answers were provided, and the case was dismissed.

As mentioned above, the discussions surrounding extraterritorial enforcement of the GDPR possibly have even more far-reaching implications – the jurisdiction model introduced there was copied also in the proposal of the EU's AI Act and the Digital Services Act. Therefore, the doubts that we express about the enforcement of decisions of EU authorities outside the territory of the EU, *per analogiam* also apply – at least in part – to these two pieces of legislation. According to the Commission's proposal, AI Act should apply to: (i) providers placing on the market or putting into service AI systems in the Union, irrespective of whether those providers are established within the Union or in a third country; (ii) users of AI systems located within the Union; (iii) providers and users of AI systems that are located in a third country, where the output produced by the system is used in the Union.[51] The draft AI Act has therefore an extraterritorial scope, which relies on the destination approach, involving targeting and market access trigger, that we know from the GDPR. What could make a difference in its case is that provisions of the AI Act shall be enforced by national competent authorities, which can be, but do not have to be data protection authorities and therefore could apply different enforcement mechanisms. However, in some Member States, such as France, it is very probable that a data protection authority will be enforcing the AI Act.[52] Also, the DSA has an extraterritorial scope and relies on targeting and the market access trigger. According to Article 2(1) DSA, it shall apply to intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment. What differs the DSA from the GDPR is that it foresees an enforcement co-shared between Member States and the European Commission and that for the case of very large online platforms and very large online search engines, the Commission will have direct supervision and enforcement powers. At the same time, competent authorities of Member States

[51] Regarding the extraterritorial impact of this, see further: Dan Svantesson, The European Union Artificial Intelligence Act: Potential implications for Australia, Alternative Law Journal 2022, Vol. 47(1) 4–9.

[52] T. Hartmann, French data protection authority lays out action plan on AI, ChatGPT, https://www.euractiv.com/section/artificial-intelligence/news/french-data-protection-authority-lays-out-action-plan-on-ai/, last access: 23 July 2023.

will supervise smaller platforms and search engines including non-EU ones, which appointed a representative in a particular Member State, or which failed to designate a legal representative.[53]

5.5 Failure to designate a representative in the EU

According to Article 27 GDPR as a principle, all controllers and processors not established in the EU whose activities fall within the territorial scope of the GDPR have to appoint a "representative"; we can refer to this as a "rep localisation requirement".[54] This requirement is not compulsory in cases described in Article 27(2) GDPR.[55] In practice, an appointment of a representative in the EU makes the GDPR enforcement much easier as it creates a contact point of a third country controller or processor in the EU that data protection authorities can reach out to. Also, an appointment of a representative enables EU residents to exercise their rights more easily, as they can contact someone located in Europe. A representative can be a natural or a legal person.

A person to be considered a "representative" needs to be explicitly designated as such by the controller or processor in writing, the representative must be able to act on behalf of a controller or a processor with respect to their obligations under the GDPR. Some Member States further specified requirements to be met by a representative.[56] Under the GDPR, a representative acts as a contact point and cannot be held liable for actions of a controller or a processor.

The EDPB summarizes the concept of the representative in the following way:

[53] According to recital 123 DSA: "(…) In respect of providers that are not established in the Union, but that offer services in the Union and therefore fall within the scope of this Regulation, the Member State where those providers appointed their legal representative should have competence, considering the function of legal representatives under this Regulation. In the interest of the effective application of this Regulation, all Member States or the Commission, where applicable, should, however, have competence in respect of providers that failed to designate a legal representative. That competence may be exercised by any of the competent authorities or the Commission, provided that the provider is not subject to enforcement proceedings for the same facts by another competent authority or the Commission (…)".

[54] See further: Svantesson, D. J. B. (2018). European Union Claims of Jurisdiction over the Internet: An Analysis of Three Recent Key Developments. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 9(2), 113–125. https://www.jipitec.eu/issues/jipitec-9-2-2018/4722.

[55] The obligation shall not apply to: (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or (b) a public authority or body.

[56] L. Tosoni, 'Article 4(17). Representative', in Ch. Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (New York, 2020; online edn, Oxford Academic), last access: 23 July 2023.

> "the concept of the representative was introduced with the aim of facilitating the liaison with and ensuring effective enforcement of the GDPR against Article3(2) of the GDPR controllers/processors. To this end, it was the intention to enable supervisory authorities to initiate enforcement proceedings through the representative designated by the controllers or processors not established in the Union. This includes the possibility for supervisory authorities to address corrective measures or administrative fines and penalties imposed on the controller or processor not established in the Union to the representative, in accordance with articles 58(2) and 83 of the GDPR. The possibility to hold a representative directly liable is however limited to its direct obligations referred to in Article 30 and Article 58(1)a of the GDPR."[57]

Kuner notes that there are few organizations or individuals offering their services as representatives, and "their reliability, experience, and solvency are often not clear".[58] This is the case in a situation where a representative cannot be held liable for controller's or processor's actions. In a situation where there would be a certain level of liability, the situation would be even worse. However, not appointing a representative is a breach of the GDPR and a quite visible signal that a particular controller or processor does not intend to comply with the EU laws. According to Article 83(4) GDPR, it is subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Although the fine for failure to designate a representative can be very significant, national data protection authorities have no effective tools that they could use to force non-EU controllers or processors to appoint a representative. Moreover, there is no procedure that would allow the European Commission or EU Member States to effectively enforce this obligation. The decision against Clearview AI and the situations described in the EDPB study seems to confirm that this is an issue.

We would like to illustrate possible problems with the representative using the example of one case conducted by the supervisory authority from Luxembourg, which was described by the complainant on his blog.[59] The DPA of Luxemburg, *Commission nationale pour la protection*

[57] Study on the enforcement of GDPR obligations against entities established outside the EEA but falling under Article 3(2) GDPR. Final report, p. 41.

[58] Ch. Kuner, Territorial Scope and Data Transfer Rules in the GDPR: Realising the EU's Ambition of Borderless Data Protection (April 16, 2021). University of Cambridge Faculty of Law Research Paper No. 20/2021, p. 27.

[59] In this paper we mention several similar cases, investigated by different DPAs, we decided to use this particular case as it was described by a complainant in a blogpost. See.T. Zoller How to effectively evade the GDPR and the reach of the DPA (CDPWE-0001) (PART 1), https://blog.zoller.lu/2020/05/how-to-effectively-evade-gdpr-and-reach.html, last access:

des donées (hereinafter: "CNPD"), is supervising all controllers located in Luxemburg, many of them being big companies benefiting from Luxemburg's tax system. This makes the CNPD one of the most important authorities in Europe, and it is perhaps best known for imposing a €746 million fine on Amazon Europe Core S.à.r.l. for violations of the GDPR.[60]

In the case we examine here, a citizen of Luxemburg found online that a US-based companies was selling access to his personal data. He lodged a data access request with the company and asked for the purpose and the legal basis of the processing. The company did not have a representative in the EU. Moreover, the company denied that they are a controller under the GDPR. The affected data subject then complained about the company to the CNPD. In their response, CNPD recalled recital 116 GDPR, which states that:

> "[w]hen personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints."[61]

CNPD also stated that "supervisory authorities may be faced with the impossibility to investigate complaints or activities outside their borders".[62] In conclusion, CNPD replied to the complainant that "we are unable to take any further action in relation to your complaint. We do not have the authority to investigate and enforce any decision we would have to take in the United States of America".[63] The violation of the GDPR therefore continues.

Data protection authorities under the GDPR, are obliged to apply the EU data protection laws. The statement that investigation is not possible due to lack of a representative seems to be difficult to justify, but are far from uncommon, and by no means limited to Luxemburg, or indeed

---

23.07.2023. This case was brought to our attention by *Contribution to the public consultation on the Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR*, submitted with the EDPB by L. Drechsler and S. Yakovleva.

60 The decision was not made public but confirmed by Amazon in their reporting to the US Security Exchange Commission: https://d18rn0p25nwr6d.cloudfront.net/CIK-0001018724/cbae1abf-eddb-4451-9186-6753b02cc4eb.pdf, last access: 23 July 2023.

61 Ibid.

62 Ibid.

63 Ibid.

to the context of EU's data protection regime. However, we argue that the GDPR obliges Member States to seek effective enforcement. In this case, the lack of actions by a DPA or a Member State could potentially lead to infringement proceedings under Article 258 TFEU.

This case, investigated by one of the most significant data protection authorities in Europe, shows that data protection authorities are not able to force non-EU entities to appoint representative in the EU. Moreover, a decision not to appoint a representative seemingly pays off – companies which do not appoint a representative in the EU have lower chances of being investigated in the EU and face penalties. This goes against one of the GDPR's stated objective, which – as noted above – was to create a level playing field for EU and non-EU actors operating in the EU market.

Examples such as this are particularly worrying as an obligation for non-EU actors to appoint a representative in the EU was introduced in several other EU legal acts. For example, under the Digital Services Act, online intermediaries established outside of the European Union that offer their services in the single market will have to appoint a legal representative in the EU. The role of a legal representative is described in Article 13 DSA and it goes beyond the responsibilities of representatives under the GDPR.[64] According to Article 13(3) DSA, a representative can be held liable "[i]t shall be possible for the designated legal representative to be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability and legal actions that could be initiated against the provider of intermediary services". In line with Article 56(6) DSA the Member State where its legal representative resides or is established or the European Commission shall have powers, as applicable, to supervise and enforce the relevant obligations under this Regulation. All Member States or, where applicable, the Commission, have competence in respect of non-EU providers that failed to designate a legal representative.

[64] Recital 44 of the DSA states that "[p]roviders of intermediary services that are established in a third country and that offer services in the Union should designate a sufficiently mandated legal representative in the Union and provide information relating to their legal representatives to the relevant authorities and make it publicly available". Recital 123 explains that "[i]n respect of providers that are not established in the Union, but that offer services in the Union and therefore fall within the scope of this Regulation, the Member State where those providers appointed their legal representative should have competence, considering the function of legal representatives under this Regulation. In the interest of the effective application of this Regulation, all Member States or the Commission, where applicable, should, however, have competence in respect of providers that failed to designate a legal representative. That competence may be exercised by any of the competent authorities or the Commission, provided that the provider is not subject to enforcement proceedings for the same facts by another competent authority or the Commission".

Also, the draft EU's AI Act involves the concept of a representative. In line with Article 25(1) AI Act, "[p]rior to making their systems available on the Union market, where an importer cannot be identified, providers established outside the Union shall, by written mandate, appoint an authorised representative which is established in the Union." At the time of completion of work on this paper the draft AI Act was in the trilogues, therefore the final wording of this provision is still not agreed.

In addition to the observations made above as to the inefficiency of the enforcement of the GDPR's rep localisation requirement, it may also be noted that the potential downsides of the rep localisation requirement have gained surprisingly little attention. Most importantly, it ought to be noted that rep localization as a response to the international nature of the Internet is not scalable. First, when other countries also adopt this approach – as, for example, is the case in the Thai data protection law[65] – businesses are going to have to have representatives in all the countries in which they are active. This clearly undermines the value of Internet-based cross-border commerce.

Second, even where the size of the EU market makes businesses accept the EU's rep localisation requirements, that does not translate well to the rest of the world. Where smaller economies adopt the same approach, will it be worthwhile for the Internet companies to have representatives in each of those states too? Most likely not. Thus, rep localization, even to the extent that it works for the EU, is not the solution for the rest of the world. And one can perhaps make the claim that, given the EU's appetite for inspiring the conduct of other countries, it could have done more to find a globally – or partially globally – viable solution. Doing so should perhaps come naturally given the stated goal of ensuring an equal playing field?[66]

To conclude the discussion of the GDPR's extraterritoriality, we note that, in May 2023, when discussing obligations imposed on Twitter and arising from DSA, Commissioner Breton stated "You can run but you can't hide".[67] Apparently, in case of the GDPR, third country controllers or processors without an establishment in the EU can run, hide and arguably too easily avoid any responsibility for violations of EU data protection laws.

[65] Thailand Personal Data Protection Act, Section 37(5).

[66] See further: Dan Jerker B Svantesson, Internet & Jurisdiction Global Status Report 2019 (Internet & Jurisdiction Policy Network, 2019) 147–8.

[67] G. Carbonaro, S. Khatsenkova 'Bye, bye birdie': EU bids farewell to Twitter as company pulls out of code to fight disinformation, Euronews, https://www.euronews.com/next/2023/05/29/bye-bye-birdie-eu-bids-farewell-to-twitter-as-company-pulls-out-of-code-to-fight-disinform, last access: 23.07.2023.

6. Conclusions

With a focus on the extraterritoriality of application of data privacy laws, the text above has sought to highlight how the legal landscape – and indeed, the world – has evolved since the Datalagen was introduced 50 years ago. The drafters of the Datalagen could hardly have imagined the immense role that data privacy law now plays for societies around the world. And it would have been difficult to predict the role that data privacy law would turn out to play in developing the EU's regulatory influence on the world.

With all the recently adopted digital laws introduced in the EU, it is clear that the European Union wants to actively regulate Cyberspace. But for this to happen, it needs to be able to enforce its laws. Almost 10 years ago, on 4 March 2014, then European Commission Vice-President Viviane Reding, when addressing representatives of EU Member States, stressed that the proposed GDPR "is about creating a level playing-field between European and non-European businesses. About fair competition in a globalised world".[68] We believe that this promise has not yet been fully delivered.

Situations where European data protection authorities admit that they struggle and lack legal tools to deal with controllers or processors that fall under the scope of Article 3(2) GDPR but are not willing to cooperate and do not designate an EU representative under Article 27 GDPR, are not acceptable and go against the GDPR. This situation seems to result in a violation of law not only by controllers and processors in question but also by Member States and their authorities. In our opinion, in line with Article 258 TFEU it could trigger a reaction against Member States from the European Commission – as it is the Commission's duty, as a guardian of the Treaties, to ensure effective enforcement of EU law. Moreover, it gives reasons to worry about the extraterritorial enforcement of other EU legal acts such as the DSA or the AI Act, which have their extraterritorial scope based on a similar moderate destination approach and market access trigger as the GDPR.

At the same time, it could be argued that provisions such as the GDPR's Article 3(2) – as currently drafted – may be overly broad in reach thus undermining the possibility of effective enforcement of the law. Put simply, Article 3(2) could be seen to result in a situation where the GDPR applies in such a large number of cases that the authorities tasked

[68] Viviane Reding, 'The EU Data Protection Regulation: Promoting Technological Innovation and Safeguarding Citizens' Rights' (Brussels, 4 March 2014), http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm, last access: 23 July 2023.

with its enforcement are set up to fail. Similar situations may arise in the context of the DSA and, in particular, the AI Act.

Relatedly, the 'levelling of the playing field' argument underpinning the current structure of Article 3 fails to recognize the fact that foreign businesses respond to the GDPR differently. While the "big players" have the resources to adjust their behaviour so as to be GDPR-compliant, that is not always the case for the small- to medium-sized businesses around the world. Some have adjusted their behaviour to the GDPR, whether they are actually subject to it or not, but many have not and carry on as usual, hoping they will not be subject to any enforcement actions. And given how many non-EU businesses fall within Article 3(2) GDPR and taking account of the resources available for national data protection authorities enforcing the GDPR, perhaps the odds are in their favour. For EU citizens dealing with such businesses, it is difficult to see the GDPR bringing any substantial improvements, and there might be no levelling of the playing field either.

Furthermore, as there clearly will be more foreign businesses failing to comply with the GDPR than there are resources to investigate them, there is a risk that the actual application of the GDPR will necessarily be arbitrary, which could arguably undermine the legitimacy of any enforcement actions taken. In this context, and also bearing in mind the large scale of processing of EU residents' data by non-EU entities, what is already worrying is a relatively small number of cases relying on Article 3(2) GDPR, despite its key role in the protection of EU residents against any data protection related external threats.

In the years to come, we will witness various new services and development of new architectures e.g., for the purposes of artificial intelligence, which are being developed by a private sector, to vast extend happens without public oversight. This was the case for ChatGPT, which was publicly released on 30 November 2022 and with its unprecedented and powerful capabilities immediately revolutionised the way in which humans use generative-AI. This, together with a fragmentation of rights and freedoms in the world, may create even more challenges in the future, as the Internet is slowly becoming a decentralised space governed by centralized powers. We witness a growing power of platforms, but also at the same time attempts by different actors, including the European Union to reterritorialize the Internet. For now, it seems that EU power lies, not in hard law, but in a soft extraterritoriality of values and the "Brussels effect". This, however, might be not sufficient in the long term. Effective protection of the fundamental right to data protection requires not only an extraterritorial scope but also mechanisms that would allow for effective enforcement of decisions issued by Euro-

pean data protection authorities. Otherwise, we risk a growing disconnection between the law on the books and its practice.

In this context, we believe that first the EU should closely monitor whether mechanisms of appointing a representative, as foreseen in the GDPR, DSA or draft AI Act, work in practice. If it is concluded that they do not work well, work is needed to assess how to either make them workable, or how to replace them. The European Union could for example explore the concept of 'market sovereignty'[69] e.g., in the form of blacklisting, on the EU level, companies that do not appoint representatives. A certain form of blacklisting – in the context of adequacy – existed already under Directive 95/46/EC (see Art. 25(3) and (4) thereof)[70] it was also present in the initial GDPR proposal, as published by the European Commission.[71] According to the GDPR proposal, the Commission would publish the list of blacklisted countries, territories, sectors and organisations in the Official Journal of the European Union.[72] Although relevant provision was not included in the final text, it shows that the concept of blacklisting is not new to EU data protection laws. A register of non-EU entities that violate Art. 27 GDPR or relevant provisions of DSA and AI Act could be made public by the European Commission and would be a clear signal to business partners or contractors that these companies or individuals have problems with compliance. We are convinced that such a tool would have a deterrent effect on non-EU entities and would help in an efficient extraterritorial enforcement of the EU laws. Measuring the appeal of such an approach must, however, also take account of the cost of other countries imposing the same type of

[69] For a detailed discussion of the concept of 'market sovereignty' supported by 'market destroying measures' such as blacklisting, see further: D.J.B. Svantesson, *Solving the Internet Jurisdiction Puzzle*, Oxford University Press, Oxford 2017, pp. 141–148; and Dan Jerker B. Svantesson, A doctrine of 'market sovereignty' to solve international law issues on the Internet?, OUPblog 5th April, 2014, https://blog.oup.com/2014/04/market-sovereignty-international-law-internet/).

[70] According to these provisions "3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2. 4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question".

[71] See Art. 41(5)-(7) of Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011 final – 2012/0011 (COD).

[72] According to Art. 41(7) of the Proposal "The Commission shall publish in the Official Journal of the European Union a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured".

rep localisation requirements on EU businesses acting outside the EU market.

Secondly, the EU may have to admit that some changes, in particular new international enforcement mechanisms, might be needed. The EU legislators and the European Commission need to stay open minded and, if needed, create new or be ready to re-assess the current toolbox in the light of globalisation and technological progress. As pointed out above, what makes non-EU companies comply with EU laws is the EU market with almost 500 million consumers that buy products and services. This is the biggest incentive for non-EU companies to follow the EU law and the EU should make use of it. The most burning challenge in the context of extraterritoriality of the EU digital laws might be the absence of tools that could be used by national or EU authorities to enforce EU law outside of its territory.

In the long term, the lack of effective enforcement arguably threatens EU legitimacy and its leading role in the interconnected, globalised world. Knowing that the EU cannot compete with China as regards "exporting" infrastructure or with the US as regards creating an environment that incentivises innovation, keeping the EU's ability to regulate the online environment is the key for the EU to maintain its role as a global norm-setter. This role will depend on its capacity to effectively enforce EU laws outside of the EU.

The world has changed dramatically over the 50 years since the Datalagen was introduced. Perhaps it can be said that the change from Datalagen's approach (no specific claim of extraterritoriality) to the GDPR's approach (detailed regulation of the extraterritorial scope) clearly reflects how the world has changed during the 45 years that separate them (1973–2018). The GDPR is tasked with addressing a much more international data processing environment, in no small part due to the Internet. And as we have sought to illustrate, the five years during which the GDPR has been the applicable data privacy law have highlighted that the GDPR's approach is already under strain; especially if it is to remain a key component in the EU's international regulatory influence.

It is far from unimaginable that the world will change, in an equally dramatic manner, in the next 50 years as it has since the Datalagen was first introduced, and the law will no doubt have to change with it.