GDPR as a Global Standards? Brussels' Instrument of Policy Diffusion

https://www.e-ir.info/2022/04/09/gdpr-as-a-global-standards-brussels-instrument-of-policy-diffusion/

MARCO LUISI, APR 9 2022

The 4th Industrial Revolution is witnessing the emergence of new digital computing technologies able to collect and analyze immense quantities of information – called “big data” – and translate this into something economically, socially, and politically valuable. Data-driven algorithms, like the one behind targeted ads, become more powerful and efficient the more private information they acquire. But the risks connected to the misuse of data have reignited the public interest in privacy and its protection. This is what Colin J. Bennett calls the “second wave of global privacy protection” (Swire, 2013: 848).

By the year 2020, 147 data protection laws have been enacted, 66 in the sole decade 2010-2020, marking an increase of 50% (Figure 1). The EU General Data Protection Regulation (GDPR) is one of these. It was published in 2016 and enacted two years later. Since then, it has turned out to be the most influential attempt to regulate data protection. As a matter of fact, the Regulation is widely considered a blueprint for data privacy, often referred to as the “gold standard” for international data usage (Buttarelli, 2016). The vast majority of these 66 laws mentioned have in some way mimicked the principles and structure of the GDPR, in a way that has interested many social scientists. This phenomenon in which national regulations become increasingly aligned with prevailing international standards is known as “regulatory convergence” (Kerr, 1983, p. 3). Academic analysis of regulatory convergence focuses on the conditions that enable the global spread of regulatory norms in general and, on the role of the EU in this matter in particular (Bradford, 2015; Young, 2015; Ng, 2019; Moravcsik, 2017).

Recently, legal convergence has been extensively used in reference to the phenomenon of global diffusion of the EU standards for data protection. In particular, both the mainstream media and the academia have referred to it as to the “Brussels Effect,” borrowing the expression from a famous work by Anu Bradford (2012) addressing this phenomenon (Bennett, 2018; Greenleaf, 2018; European Commission, 2019; The Economist, 2021).

The existing literature agrees on the impact that the EU is having in shaping the global norms for data protection and supports the idea of a Brussels Effect. However, it fails to discuss the substance of it. This happens either because the studies predate the GDPR, or because subsequent studies still base their conclusions on that same primary literature. Paul M. Schwartz (2016), for instance, pointed out the lack of a coherent set of data protection norms to export, and thus the complete absence of the conditions for a *de jure* diffusion. Daniel W. Drezner (2007), on the other hand, maintains that state regulations could possibly do nothing against the misuse of personal data by internet sites operating offshore. Both, though, wrote before the GDPR was a thing, or before the State of California could enforce its GDPR-like data protection law (the CCPA), proving the authors to be wrong. For this reason, further research on the current mechanisms behind the spread of the EU standards for data protection is desirable.

This research, therefore, assesses the relevance and explanatory power of Anu Bradford’s Brussels Effect with respect to the regulation of digital privacy by the EU and its diffusion globally. It concludes that the theory is a valuable analytical approach for understanding the mechanisms of externalization of the EU data protection norms. In particular, drawing upon new empirical data this research bolsters the argument that the regulatory instrument deployed by the EU – the GDPR – does influence the behaviors of foreign companies and governments as well, through their dependence on access to the European Single Market. Ignoring the digital privacy of the European

citizens, in fact, would pose huge risks to the non-EU actors that regularly work with big data (virtually all organizations, commercial or not), jeopardizing their profits and threatening to exclude them from the biggest consumer market in the world. This market power eventually results in a regulatory convergence towards the European privacy standards, which takes place both in the forms of formal enactments of privacy laws by national jurisdictions and informal application of EU-inspired corporate codes of conduct.

Chapter One: Research Design and Methodology

This research is built upon the evidence of a convergence of the global standards for data protection toward the GDPR model established by the EU. The main question that it attempts to answer is does the Brussels Effect convincingly explain the reasons why the EU data protection regulation is being adopted as a global standard and thereby evidence of global regulatory convergence?

The methodology adopted to answer this question is that of Process-Tracing (PT). This methodology investigates the causes that led to a specific outcome (Beach, 2016). It is often adopted in social science to test existing theories based on causal mechanisms like many regulatory convergence theories normally do (Beach, 2016, pp. 463-464). It goes without saying that the main hypothesis is that regulatory convergence of data protection norms is caused by the "Brussels Effect". As argued by Beach (Beach, 2016, p. 464), for this methodology to be effective, the researcher first needs to "[unpack] causal processes linking X and Y". In practice, this means dissecting the mechanisms of convergence found by Bradford (the conditions) to make them easily assessable from an analytical and empirical perspective. The method, therefore, is applied by analyzing the conditions of *de jure* and *de facto* convergence, and then identifying empirical observables that can prove the hypothesis correct or wrong.

The Brussels Effect claims that the EU can induce convergence mostly through market mechanisms – in a process that she refers to as "unilateral regulatory globalization" (Bradford, 2015). The peculiarity of this type of convergence lies in the fact that the EU laws are remarkably very strict and onerous, making their replication elsewhere daunting. Nonetheless, the evidence shows a process of Europeanization of international and foreign domestic law. The push towards convergence is induced through the Single Market, access to which, being economically profitable for many, is worth foreign companies complying with its rules (Bradford, 2015, p. 159). But what makes compliance and trading up truly possible is the combination of the EU's regulatory clout and of unavoidable technical and economic constraints. Basically, strictness and iron fist in the enactment and enforcement of the law, and impossibility for companies to water down or circumvent the law in any way (Greenleaf, 2012). These factors eventually result in a) the *de facto* Effect, in which multinational companies abide by the EU law to maintain their access to the Single Market; and b) the *de jure* Effect, in which the same multinational companies lobby against their domestic governments to level the playing field (Bradford, 2015, p. 159). In other terms, non-EU jurisdictions would feel forced to formally establish rules that echo the European ones to satisfy the growing demand for equal competition and conditions.

How can these causal links be translated into empirical data? The logic of the laws of non-contradiction assists with this. This inquiry was structured as a series of counterfactual conditionals that challenge the basic axioms of the Brussels Effect. For the postulate "convergence = Brussels Effect" to be likely, one should adduce some evidence that the convergence is actually taking place due to market mechanisms. If this is not true, or there is not enough evidence for this to be plausible, then, advancing such a hypothesis would be impossible to begin with. At the same time, though, even in the case of formal evidence of market incentives behind convergence, I examine the possibility that other major conditions could be present to trigger the occurrence of the Brussels Effect.

This inquiry test the very basic assumption that a regulatory convergence towards the EU standards for data protection is actually occurring. The test is modeled upon a previous study by Graham Greenleaf (2012). In his study, he first identified a series of 10 data privacy principles stemming from the EU law, which he named "European elements" (Greenleaf, 2012). Then he embarked on an a-historical analysis of 33 non-EU data protection laws drafted or enacted since the enforcement of the Directive 95 to assess whether these embodied at least some of these principles established by the EU. The results offered evidence of the influence exerted by Directive onto the other national laws since its enforcement and, most importantly, allowed the author to express in numbers such a

convergence (Greenleaf, 2012).

This study applies the same method on a sample of 58 non-EU national privacy acts published and enforced between 2016 (the year the GDPR was published) and 2020. The timeframe appears drastically shorter than the one opted by Greenleaf. This however is counterbalanced by the higher concentration of legislations issued in this shorter period. The parameters for comparison were increased to 11 to include the appointment of a Data Protection Officer (DPO), which is arguably another key element that distinguished the GDPR from the previously existing frameworks. The remaining 10 are consistent with the Greenleaf (2012) study. These are: 1) appointment of an independent Data Protection Authority (DPA); 2) possibility to appeal to a court to enforce one's privacy rights; 3) sufficient measures of data protection for cross-border data transfer; 4) principles of purpose limitation and data minimization; 5) a general definition of what does it mean to collect and process data fairly and lawfully; 6) requirement to notify the Data Subject and/or the Authority about the processing of data; 7) principles of data retention; 8) additional measures for sensitive information and children's data; 9) limits on automated decision making; 10) right to "opt-out" of collection and processing for purposes of direct marketing (Greenleaf, 2012).

The analysis uses official texts of the acts available from different sources, namely UNCTAD, DLA Piper, and WorldLII (UNCTAD, n.d.; WorldLII, 2022; DLA Piper, 2022). The results made it possible to quantify the degree of convergence towards the GDPR, from the lowest score, 0 elements in common, to the highest, 11. From a broader perspective, it was also possible to evaluate the trend of convergence occurring since the previous study, expressing the results of both in terms of standard deviation from the current European law examined. The scores of the single jurisdictions were also cross-checked with further statistics on the trade in online data and services between the EU and the different nations. As well as with data on the political environment in one specific country. That way it was possible to add a second layer of comprehension to the mere numeric data, and perhaps interpret the main reasons behind one specific score. The comparison is displayed in Table 1 in the Appendix.

The second aspect of the methodology addresses one by one the conditions (or prerequisites) Bradford (2015) argues are associated with regulatory convergence. The object is to deduce correlations between the occurrence of these conditions and the diffusion of the EU data privacy norms. According to the Brussels Effect, the worldwide spread of strict European standards is the result of 1) the economic significance of the Single Market such that it is commercially disadvantageous not to conduct business in this market; 2) high regulatory capacity and internal incentives for the enactment of stricter norms; and 3) the impossibility for companies to either circumvent the law or pursue double standards (for reasons of non-divisibility or because relocating under different jurisdictions would not change the situation anyway) (Bradford, 2015, pp. 158-161). This series of analyses were more qualitative, mostly based on the consultation of secondary and primary sources including scholarly and newspaper articles, government publications, interviews, and public statements.

Chapter Two: De Jure Convergence: What the Figures Tell about Convergence

The initial comparison of the 58 data privacy acts (49 laws and 9 bills) ultimately led to the following conclusion. The number of new privacy laws has almost doubled during the last decade, such that European laws no longer represent the majority. Remarkably, since 2016 the scale of regulatory initiatives for privacy has been unprecedented as shown in Figure 2. This suggests that the GDPR may have played an active role in prompting a global race to data protection.

More significantly, the 58 acts published during this timeframe show a high degree of correspondence with the GDPR. Comparing this result with the study by Greenleaf, it is also possible to conclude that this convergence has increased over time. For clarity, the degree of convergence was expressed in terms of average incidence rate and standard deviation as well. The first statistic tells how frequently a specific element in the given sample is; the second one reflects variability in the distribution of the European elements (the average distance of other laws from the European "standard"). The average incidence is 84%, higher than the 70% incidence in Greenleaf (Greenleaf, 2012, pp. 75-77). The standard deviation is $\sigma = 1.74$, showing lower variability from the standard than in Greenleaf's 2012 study ($\sigma = 2.75$).

The results were further complemented with data from Eurostat (Chowdhry & Moes, 2018). Once merged, these ultimately seem to suggest that the highest levels of convergence with the GDPR are amongst those countries with proportionally deeper economic and diplomatic relations with the EU; or by those that at least share similar social and political principles. On the contrary, scarce digitalization, low share of trade in goods and services with the EU, and low democratic performance are all indexes of lower convergence.

These combined findings are consistent with the assumption of a regulatory convergence and associated correlation between this and economic incentives. This, ultimately, suggests that the EU market plays a significant role in this convergence and what Bradford calls a *de jure* Brussels Effect. At the same time, though, these findings provide little insight into the actual mechanisms that produce this convergence, inviting deeper research into the forces that turn the EU market into an unavoidable instrument of privacy standards exportation. This is the rationale for analyzing the conditions for convergence, from which it is possible to understand and draw conclusions about the relative significance of different casual mechanisms.

Chapter Three: An Evaluation of the Conditions for Convergence

The empirical findings backed the hypothesis that the *de jure* Effect can effectively be the manifestation of the Brussels Effect. This part, instead, evaluates the conditions identified by Bradford that can translate economic interdependence into a *de facto* Effect.

3.1. Market size:

This first analysis focuses on the assumption that the Single Market could trigger the diffusion of data protection norms. The reason why market size (the cause) and convergence (the effect) would be related had been addressed long before by a rich scholarship. Market Power theories, for instance, are mostly built on this assumption (Damro, 2012; Drezner, 2005). Chad Damro states that the normative power of the EU and its ability to externalize its standards would, in practice, root in its Single Market (Damro, 2012, p. 7). The process of convergence, in this case, occurs unintentionally with the main incentive being the market size (Damro , 2012, pp. 5-7).

Bradford, though, correctly notes that the sole consumer-base of the Single Market falls short of fully capturing the alluring effect that this market has on foreign companies (Bradford, 2012, p. 160). In fact, both China and the US appear to be stronger on paper. The two of them account respectively for 1.4 billion and 325 million citizens, all potential customers. In practice, though, China's average GDP per capita PPP in 2019 was estimated to be around $16,000 (less than half of that of the EU in the same year), and its wealth remains skewed towards the Eastern part of the country (Trading Economics, 2021a). On the other hand, the US is the world-first economy, with a GDP per capita PPP of $62,630 in 2019 (Trading Economics, 2021b). But this appears again to be unevenly distributed across the country, whereas its consumer market reveals a number of troubles for companies that must deal with a patchwork of different economic and privacy standards, minimum wages, and a plethora of local taxes.

The EU Single Market is right in the middle. 450 million people contribute to a vibrant, diversified market, and a profitable aggregator of supply and demand, all in a context of more even regulation and higher predictability for all the competitors. The EU is the world's first good and service trader, the biggest source of exports for 80 countries in the world and, remarkably, the first trader in services for the US, while the first in terms of manufactured goods for China (Damen, 2021; European Commission, n.d.b). Put in another perspective, in 2019 the EU alone accounted for more than 20% of the quarterly revenue of Facebook (Facebook, 2019). In the same year, the EU accounted for almost 20% of the US total exports in services and goods, equal to $467.6 billion (2.2% of the total US GDP in 2019) (World Bank, n.d.).

Faced with these figures, it is imperative to take into consideration the role the European market has for both governments and companies. The acknowledgment of this role is the key to understanding the Single Market strategy and the persuasive power that it has in diffusing European rules outside its legal borders.

3.2. Regulatory Capacity and preference for stricter regulations:

Bradford argues that market size alone is necessary but not sufficient for regulatory convergence to occur. The enforcement of strict data protection regulations represents a challenge for both the authorities and the society as a whole. Lack of regulatory expertise and agency, or insufficient stimula for pursuing higher standards may result in the trading down of the norms. At the same time, those subjected to the law, and even more those who are not, shall feel incentivized to abide by it, in seek of advantages and fair competition, or in fear of punishments. A large but chaotic market remains unpalatable, haunted by free-riders able to avoid the scrutiny of the competent authorities. In absence of international standards, the voices from the EU may remain mostly unheard (Bradford, 2015).

The focus on regulatory capacity and propensity for stricter regulations remains meaningful in this context even though Bradford mentions them. As also highlighted by other theories (Normative Power and Regulatory Competition theories in the first place), the perception of authority and the raising of the regulatory strictness are agreed-upon causes of regulatory convergence (Gerrits, 2009). As an example, one report issued by BRICS countries in 2019 brings up the lawsuits launched by the European Commission against Amazon and Google defining these as interesting legal precedents to study (CADE, 2019). These countries also recognize the challenges posed to smaller markets by global tech giants, and claim to be genuinely interested in learning "how the larger, more established jurisdictions […], view the competition and regulatory challenge" (CADE, 2019, p. 148). China represents another meaningful example of this correlation. The 2018 Specification is an example of legal transplantation aimed at compensating for drafters' inexperience in matters of data protection (Zhao, 2018). Quoting, the guidelines "show strong signs of convergence with the EU standards" (Pernot-Leplay, 2020, pp. 77-78).

The assessment of the EU regulatory clout is assessed here by the means of official publications of EU bodies, further complemented through academic inquiries on the EU regulatory structure. The sources shed light on a well-oiled and highly efficient bureaucratic system made at its core of over 32,000 people (European Union Employment Advisor, 2020). Almost 70% of these completed a post-graduate course, is polyglot, and more than half studied in at least one different nation (Kassim et al., 2013, pp. 39-40). 80% of the officials identify themselves as "supranationalists" and declared to have joined the EU for contributing to the cause of the European integration – which is surprising considering that the EU exists as a conglomerate of sovereign states with procedural autonomy (Hooghe, 2011, p. 101).

The number of officials employed at the EU is relatively scant, even if compared to the numbers of smaller Member States. However, the single states are not necessarily in direct competition with the EU but rather represent a further source of strength in the process of capability-building of the European regulatory power. The sources of personnel upon which the EU institutions draw are states with very high standards in terms of quality of education, with an efficiency of the public administration around the highest in the world. In practice, the regulatory capacity of the EC can be conceived as the sum of the capacities of all the single states put together. Article 296(1) TFEU, in effect, states that "Member States shall adopt all measures of national law necessary to implement legally binding Union acts," in practice delegating the burden of enforcing laws to the national authorities (Bux, 2021, p. 5).

As for the regulation of privacy and data protection, the EU has the world-largest numbers, staff-wise. It has 3535 people employed at the Data Protection Authorities (DPAs) offices in 2019 (sorted by common personnel and tech specialists) (Statista, 2020). DPAs of the European countries are also those who receive the highest budget in the world, excluding North American authorities (Fazlioglu, 2018, pp. 5,7-9). Those of staff and budgets are two key factors that have been correlated with authorities' propensity for legal actions against misuse of data (Massé. 2020, pp. 9-12). France alone, in 2017, fined Facebook €150,000 for having tracked users' data for targeted advertising (Gibbs, 2017). Google itself has a long list of fines signed France due to insufficient legal basis for processing. The lawsuits cost them over €200 million between 2019 and 2021 and, remarkably, targeted both Google LLC and Google Ireland Limited thanks to the GDPR "one stop mechanism" that extend the jurisdictional scope of states' authorities in case the violation is committed from another Member State (CNIL, 2022; Enforcement Tracker, n.d.).

What makes the enforcement of the law truly effective is the branching system of independent authorities deployed throughout the territories of the Member States. These, in turn, can exert control over data-driven companies thanks to a mandatory figure known as Data Protection Officers (DPOs). These experts, introduced with the GDPR, work in the companies in complete independence from the directors, advising on matters of data protection and referring to

the national authorities of any violation or non-observance.

At a legislative level, the quality of the procedures is sought by dividing the Commission into departments with sectorial competence, known as Directorates-General (DG), similar to national ministries. The DG Connect, responsible for the Digital Agenda does not formulate policies related to data privacy by itself. Instead, throughout the entire process, it is supported by a series of independent – also economically – and highly specialized bodies. The first is the European Data Protection Board (EDPB), formed by representatives of the national DPAs plus the European Data Protection Supervisor (EDPS). Its role is to promote harmonization and consistency in the application of the GDPR throughout the EU on the means of guidelines and best practices. It also issues opinions addressed to the EC when technical advice is needed, or a new issue related to data protection emerges. Other relevant institutions are the Secretariat, a unit made of experts in law, communication, and IT, and the European Union Agency for Cybersecurity (ENISA). Their primary role is promoting efficiency and filling potential gaps with their expertise. But Agencies like the ENISA also actively contribute to the capacity building of the EU regulatory power in other ways – like sharing their knowledge with the Commission and offering a platform for discussion between Member States and various interest groups (like the Annual Privacy Forum) which is crucial for a correct "impact assessment" analysis right before any process of policymaking (Gornitzka & Sverdrup, 2010, pp. 62-65; Eumonitor, n.d.).

However, technical competence and sufficient resources are not enough to determine the enactment of strict rules and their spread throughout the world. Vogel (1995) imagines the process of policymaking as an equilibrium between diverging forces: those who prefer lenient rules and those who want to push the bar a bit higher. Governments often have to properly weigh them before ruling over one issue that can arguably be unpopular with many. The controversy mostly derives from the economic impacts that stricter regulations alone may impose on the market (Guasch & Hahn, 1999). This is all the more true for data protection. The average costs of GDPR compliance for firms are higher than $1 million in the US (PwC, 2017). These costs must be combined with those of maintenance as well. Even in wealthier countries, this means increasing the prices of online services to cover the costs of compliance – which can represent a blow to the competitiveness of many businesses. SMEs may simply see their access to the digital market completely negated due to a lack of liquidity or expertise. For others still, having to divert their profits almost entirely towards the costs of compliance and maintenance represents an impediment to innovation (McQuinn & Castro, 2019).

And yet, the GDPR is a thing, and its diffusion is happening. Such propensity finds its explanation in different reasons. The first one is internal. Several Member States have shown a propensity for regulating specific policy areas of their interest, developing in the meanwhile reputation and experience in the field. These can gain leverage through their competence in the form of external assistance and are directly interested in advising bodies like the EC to see their own laws and practices extended to the whole Union in a process of harmonization (Gornitzka & Sverdrup, 2010). In this regard, Tobias Arnoldussen theorizes that certain critical events may induce states to uphold a cause, legislate by their own first, and then try to involve other nations by appealing to the European institutions to force a regulation that comes from above (Arnoldussen, 2019). The aforementioned Agencies, in fact, may function as important channels for Member States to instruct the European legislators and directly influence the drafting of a policy. Germany is an example of this. It holds the record of the world's first data protection law, enforced in 1970, and is also mentioned for its 1983 Population Census Decision which resulted in the Right of Informational Self-Determinism – deemed to be the progenitor of the GDPR's "right to be forgotten" (Kodde, 2016, pp. 1-2). French, too, had its first laws passed in 1978. The legacy of these two legislators is still visible today in the GDPR, and in its precursor, the Directive 95. The concepts of human dignity embodied in the German law, and that of personal integrity present in the French one, after all, hint at the role that these two countries had in the drafting of the Community law. The same *pro-fundamental right* twist took place mostly under the directorship of these two Member States and was further facilitated under the post-Lisbon Treaty regime (Molnár-Gábor, 2018).

The Commission, on its side, can "profit from the experience obtained by Member States" to legislate more consciously and ultimately level the playing field "via Community legislation" (Rüdiger, 2006, p. 77).The incentives to raise the European laws at the levels of the most zealous regulators can be attributed to one objective necessity and to a plausible guesswork. First, the EU needs to stay faithful to the principles of the Single European Act and not

undermine the free flow of goods, services, and data throughout the Single Market. Secondly, the fame itself of being a "normative power" may impose a strong pressure on the EU, forcing it to act coherently, especially if it comes to privacy, that is a human right as according to articles 7 and 8 of the EU Charter of Fundamental Rights (Charter of Fundamental Rights of the European Union, 2000, p. 10). As a matter of fact, only Austria rejected the text of the GDPR at a certain point of its drafting but, surprisingly, because not strict enough for their standards (General Secretariat, 2016). A thing that, eventually, was taken into consideration in the final version of the Regulation, that now contains opening clauses allowing the single Member States to introduce additional provisions to enhance the scope of the law, as long as they do not undermine the free flow of data within the Single Market (European Union, 2016). Members in a condition of minor strength and wealth did not oppose the GDPR, confident that they could even benefit from it. And, in fact, they can easily tap into extra funds and know-how to compensate for the implementation costs and lack of expertise. Between 2017 and May 2020, for instance, the EU, by the means of the national DPAs, organized and funded 19 projects aimed at easing the introduction and implementation of the new technical requirements under the GDPR. Most of these activities targeted the most sensible groups, namely individuals – often unaware of their digital rights – and SMEs (European Commission, n.d.a). Other activities took the form of training meetings organized by the DPAs and intended for other DPAs (Cataleta, 2019).

The final incentive for the enactment of such a strict data protection framework comes from below. More exactly from the citizens and the market itself. Complying with the GDPR comes with evident economic burdens, but several advantages as well. The Regulation is desirable for firms and individuals because puts them in front of a single set of rules evenly enforced and that work consistently throughout the entire Single Market. Moreover, its severe, catch-all approach to data protection makes being GDPR-compliant a way to have access to every other market in the world, without having to adjust one own business model. The GDPR also pushes firms to keep updated and well-ordered their databases, to store as little data as possible, and to delete outdated or unused ones. This benefits data management and even plays a role in marketing strategies, providing high-quality leads, and increasing ROI (Mitchener, 2002; The Wall St. J., 2007). As importantly, GDPR-compliance can be leveraged by companies as a symbol of commitment to their customers' privacy. As privacy becomes a requirement that can be proudly showcased, it is being witnessed the emergence of a new business culture that revolves around showing off the most sophisticated measures of data protection. European citizens, for instance, frown upon the usage of their data for commercial purposes, preferring those companies that are explicitly committed to protecting users' privacy (ComRes, 2015). Companies seem to have taken note of this. From Zuckerberg to Tim Cook, the CEO of Apple, many important entrepreneurs are backing the European framework. Mark Zuckerberg, for instance, testifying before the House Committee on Commerce and Energy, announced that Facebook planned to extend the same level of protection set by the GDPR globally (Jeong, 2018).

3.3. Regulation of inelastic targets:

This third analysis shifts the focus to the companies involved in the digital economy, and how these eventually contribute to the diffusion of the EU data protection norms.

In traditional capital markets, firms can exploit de-regulated regimes to economize on the costs and sell their products or services at a competitive price there where stricter regulations induce a raise of the prices – in the same way as shipping companies can operate under different flags without compromising their access to other ports. Often these escamotages harm the quality of the policies enacted by jurisdictions. Laggards-on-purpose will decide to set out their regulations to incentive the relocation of productions from abroad. This phenomenon is generally known as "the Delaware Effect," and is the natural counterpart of the "California Effect" and of the Brussels Effect as well (Coffee, 1987). Drezner points out that the Internet would be subjected to the same dynamics, "making it theoretically possible for business and individuals to bypass bothersome regulations" (Drezner, 2007, p. 91). Then, he added "[i]t seems difficult to reconcile state regulations with the decentralized structure of the computer network", referring to the scant incentive to regulate the Internet in the face of easy way-arounds (Drezner, 2007, p. 91). As a matter of fact, Article 4 of the Directive 95 clearly stated that the law is applied to any data usage taking place within the territory of the Member States (European Union, 1995). This made it easier for companies to bypass the regulation by relocating offshore, therefore operating at a precautional distance from the EU, as Drezner argued before. The ability to relocate a business to circumvent certain rules without losing access to the international market is what

makes the target of the law "elastic." Bradford considers this the main weakness of regulatory convergence because it annuls any motive in regulating in the first place.

The GDPR, though, was designed to patch over this issue, implementing – for the first time – extraterritorial measures to the traditional data protection law. Differently from the Directive, articles 3(2)(a) and (b) of the GDPR apply to any good or service involving the usage of personal data irrespective of whether the data controller is or is not established in the Union as long as the data themselves refer to a citizen of the EU. The same standard is applied in reverse. Non-EU citizens can appeal to the European authorities if the company processing their data is in the EU (European Union, 2016, pp. 32-33). The effectiveness of the GDPR lies exactly in the fact that it targets nationality and both temporary and permanent addresses. These two things can hardly be manipulated or transferred, whereas data subjects cannot be physically brought outside the EU. Companies, therefore, cannot circumvent the law and are forced to comply with the GDPR. This is what Bradford refers to as regulating "inelastic targets" (Bradford, 2012).

To be fair, this second label may also be inappropriate. Subjects, and more specifically their data, at the current stage of the technology, are not *entirely* inelastic and do not even fall within the category of traditional consumer markets. Here it was opted to rename them "hybrid targets". Multinational companies operating both in the EU and outside will never be completely able to avoid the material scope of the GDPR. However, a way exists to ease the burden of data processing under the GDPR, and that is moving part of the targets under a more lenient jurisdiction. This strategy consists in establishing infrastructures dedicated to the sole processing of data of subjects who are neither resident in the EU nor directly EU citizens. The GDPR, in fact, does not extend to those activities which do not involve the EU territory or an EU citizen in any way during the process. For example, if a US citizen generates in Ohio data that are processed from California. Moving non-EU data under more lenient jurisdictions will not exempt companies from complying with the GDPR but at least make them legally responsible for fewer users.

For example, in 2008, Facebook established its registered office in Dublin. This was legally responsible for all the non-US users, mostly to benefit from the Irish low corporate taxes. After the enforcement of the GDPR, though, Facebook Ireland Limited became liable for misuse of personal data for over 2/3 of their global userbase. This happened because, under article 3(1), the Regulation applies regardless of the place of processing as soon as the company is registered in one of the Member States (European Union, 2016, p. 32). That same year, the company announced that they would have moved more than 1.5 billion non-EU users under the responsibility of the American subsidiary, Facebook Inc. (in Menlo Park, California) (Hern, 2018). The measure allowed Facebook to significantly reduce its exposure to the higher fines prescribed by the EU law. It was repeated in 2020 when moving UK residents under the US privacy laws became possible due to the Brexit. And even Google took a similar action that same year (Menn, 2020).

But ultimately, as long as companies are involved, even just in part, in the European market, they still have to comply with the GDPR. This strategy appears to be a mere gimmick available to big companies to avoid the high fines of the GDPR. However, as soon as other jurisdictions enact EU-like standards for privacy, firms' share of "elastic" data slowly shrinks. Shortly after moving part of its users under the Californian jurisdiction, Facebook saw the latter enacting a GDPR 2.0, and by March 2019, eleven more American states had already proposed new bills which mimic either the GDPR or the CCPA (Jeanite, 2019).

3.4. Non-divisibility of standards:

This final condition is not different from that of inelastic targets. Bradford considers it as a mandatory condition for regulatory globalization to occur, simply because it would put companies in a condition to "take it or leave it" (Bradford, 2012, p. 5). Overall, she draws up three different types of non-divisibility of standards: namely (1) legal, (2) technical, and (3) economic. Her earlier publications are eloquent about how fast new technologies permeated and influenced our societies. In Bradford 2012, she defined privacy and data protection as matters of technical non-divisibility. More specifically, she referred to a 2010 lawsuit against Google, in which the company decided to ultimately amend all their activities to the stricter European requirements because the current technology did not support data localization (sorting individuals by their residence and therefore dividing the process of data storage) (Bradford, 2012, p. 18).

However, what happened to Google seems today less likely to return. National interests succeeded in realizing what companies alone were not eager to, dividing the Internet (Crews, 2001). Today, systems like geo-blocking can sort users on the basis of the geographical position, obtained through their IP. This tool also allows companies to limit or completely impede access to their content or services from blacklisted countries. This, together with large deployments of infrastructures in different regions, finally makes it possible to localize databases and services according to and into specific jurisdictions to meet local security and data protection standards (Crews, 2001). In concrete, however, neither geo-blocking nor data localization seems to have attenuated the influence that the GDPR exerts on the global online market. The old technical non-divisibility was overcome just to be quickly followed by new obstacles and pressures that contribute to keeping the European standard more alive than ever.

3.4.1. Privacy-by-Design and by-Default: a new way to impose technical non-divisibility

From a purely technical perspective, it is not feasible to produce the same product with different privacy settings to comply with a plethora of divergent national requirements. Creating a completely separated production chain exclusively for one market would be economically unsustainable for many. It is also unreasonable to predict the nationality of the data subject that will make use of one specific smartphone, or the handing over of that same product to a data subject that falls under the GDPR.

Bradford writes that the Effect would only occur under the condition that companies convert their entire production or service according to the same, strict standards (Bradford, 2012, p. 17). Article 25 of the GDPR seems to work in this sense, profiting from the limitations mentioned right above. It forces companies that sell in the EU to embed instruments of data protection inside their products, which conform with the principles of data protection by default and by design. In theory, this does not apply to businesses not targeting the European data-subjects. However, for multinational firms which sell their products and services globally (EU included), sticking with the European standards of security during the whole production line – from the designing process to that of effective production – remains necessary.

Such an imperative explains Silicon Valley Champions' shift of business model. Apple and Google both adopt global privacy policies and terms of service that appear to be modeled upon the articles of the GDPR (as made clear, for instance, by the reference to Article 6 "Lawfulness of processing" in Apple's, and the treatment of publicly available information as "personal" in Google's, both of which have no equivalent in the CCPA) (Apple, n.d.a; n.d.b; Google, n.d.a; n.d.b; Houser & Voss, 2018, p. 27). Hardware developers like Apple and Microsoft, directly mention the implementation of privacy measures by default and by design in their products (Microsoft, n.d.; Apple, n.d.a).Amazon's intelligent virtual assistant Alexa is referred to by the company as "*designed* to protect your privacy," and the company's policy for data retention cites several principles of the GDPR, such as data minimization, the possibility to revoke one's consent, and even to erase all the recordings (Amazon, n.d.a; n.d.b).

Overall, it is interesting to witness how privacy has become a sort of "optional" to include in one's product. At the same time, the examples mentioned all come from leading multinational companies, and give an idea of the degree of the pervasiveness of the GDPR, which induces even the biggest players to design new products keeping in mind the European standards. The fact that even big multinational companies with billions in revenue cannot pursue double standards represents evidence of technical non-divisibility and, arguably, a manifestation of a *de facto* Brussels Effect (Pagallo, 2016, pp. 406-408).

3.4.2. Privacy has also become a factor of economic non-divisibility

Even assuming the possibility to pursue different standards according to the targeted markets, studies have shown a correlation between the provision of uniform standards of privacy across the markets and positive brand reputation, customer loyalty, and trust (Vogel, 2012, p. 16). In the context of growing threats to privacy and demand for security online, embedding measures of data protection into one company's business and extending them to every market – even those where such measures are not required – can remarkably reduce the level of risk perceived by consumers and assure a competitive advantage over those firms who cannot make the same vow (Cavoukian & Jolly, 2018; Doig, 2016; Strzelecki & Rizun, 2020). For well-established multinationals like Apple, which make the privacy of their

users a matter of brand identity, it would be self-defeating to apply the best measures selectively and divide their userbase into first and second-class customers. Another remarkable example comes again from Facebook that, even after moving their users under the responsibility of Facebook Inc., pledged to extend the GDPR data protection measures to each of their users regardless of where they come from (Ingram, 2018). This last case supports the previous conclusion that even though certain divisibility is still possible, this is yet undesirable.

3.4.3. The last piece of the puzzle: do SMEs have a choice?

At this point, one might wonder how all this applies to smaller, domestic-oriented businesses outside the EU. The diffusion of data protection norms among these is undoubtedly linked to the fact that much of the actions performed online take place on web browser software and are mediated by search engines like Google or Bing.

Let's consider for instance that, as in August 2021, Chrome accounts for almost 65% of the global browser market share, Safari (Apple) for 18.8% (Statcounter, n.d.a). In terms of search engines, Google operates in a condition of complete monopoly, accounting alone for 92% of the global market (Statcounter, n.d.b).

Why are these numbers so important? The answer is that data-driven businesses are subject to significant economies of scale and scope (Gal & Aviv, 2020, p. 2,8). Once a company obtains the subject's consent for processing, the same consent is automatically extended to all the internal units working for that company. This means more control over the entire process of data usage and less ping-pong of assigning responsibility between different controllers and processors. The consent also extends to all the further services offered by the company that involves that same piece of information. This reduces the costs of obtaining another consent and the number of requests submitted to the user. Finally, companies are also accountable for every data processing conducted by third parties on their behalf, creating an atmosphere of legal uncertainty and distress over the possibility that one of them might commit an infringement (GDPR, 2016, pp. 49-50, 81-83). These reasons make it more secure to entrust one's webpage or online business to one single large web operator like Google, rather than many smaller third parties. But this also implies that to start a business online, one shall first go through one of these monopolists.

These same noteworthy names, frequently under the scrutiny of the EU, have become the main tool of policy diffusion in this sense, canalizing any potential client on their platforms toward the same standards for data security and privacy. This was confirmed by Peukert et al. who monitored the "unintended effects" generated by GDPR onto several data-dependent markets – like analytics and marketing – in the months following the enforcement of the law (Peukert et al., 2020). These effects are 1) an increase of the first-party cookies vs third-party, because these guarantee more control over the collection of data and reduce the parties involved; 2) an increase of the market share of major website-hosts like Google or Microsoft, which already are GDPR-compliant; and 3) the highest levels ever of data protection compliance among US companies as a result of the fact that these lean on the former mentioned big website providers (Peukert et al., 2020).

To understand why this process of alignment with the GDPR takes place, it is important to remember that under Article 82 of the GDPR, processors (the service provider) can, under certain conditions, be held co-liable for misuse of data (GDPR, 2016, p. 49). They are consequently incentivized to promote lawfulness and transparency on their platforms and services. This is achieved, for instance, through certification-tracking systems that immediately communicate to the user if a website has implemented an HTTPS protocol. HTTPS guarantees that data are moved not in the form of plain texts but encrypted, thanks to SSL and TLS cryptographic protocols. The failure to provide one of these results in the displaying in the URL of a warning message that invites the user not to enter any personal data. In this respect, Microsoft and Google literally deployed discriminatory actions against laggards. The first introduced a browser extension that automatically detects non-HTTPS compliant and blocks them. Google, instead, deployed an algorithm-based system that exposes websites' data protection deficiencies and downgrades them, reducing the possibility to bump into an unsafe webpage when using Google or Android's searching engine (Google, 2015).

Strzelecki & Rizun found a positive correlation between the presence of HTTPS protocol and the users' willingness to perform a purchase on a given website (Strzelecki & Rizun, 2020, pp. 13-14). The discriminatory actions employed

by Google and other providers represent a threat, especially for e-commerce firms, that find themselves forced to adopt instruments of data protection for their online business even though they do not sell in Europe and do not aspire to (Strzelecki & Rizun, 2020, p. 10). Their comparative study conducted on 40 Polish online retails and 40 Ukrainian ones showed how they both had the same security protocols and data protection measures (those required by the GDPR) despite the fact that Ukraine is not in the EU, showcasing the effects that privacy protocols certifications have on the reputation of smaller online businesses and how web browsers are fostering the convergence towards the EU data protection standards even where the regulation should not apply in practice (Strzelecki & Rizun, 2020, p. 12).

According to Bradford, the Brussels Effect starts off with the main companies adhering to the EU standards and ultimately spreads across smaller domestic-oriented companies. The last three sections have shown that technical and economic non-divisibility can explain why Big Tech Monopolies decided to abide by the GDPR. The last ones have also been responsible for forcing domestic companies to apply the same measures to stay competitive, or simply to have access to the services they control. The fact that big and small companies together would operate under a regime of GDPR-compliance (even by the means of privacy-by-design approaches) can be deemed to be evidence of a *de facto* Brussels Effect.

Chapter Four: Conclusion

Whatever we decide to call it, a phenomenon of regulatory convergence in the field of data protection has been taking place steadily since the end of the XX century. It is rooted in the global recognition of privacy as a human right and revamped recently – moving in parallel with the current wave of digitalization and animated by the numerous scandals linked to the misuse of users' personal information. Moreover, the vague definition of data, their intangible nature and yet, undeniable value, makes them difficult to regulate by the means of domestic laws, encouraging the creation of complex regulatory architectures of universal ambition, able to spread outside the traditional jurisdictional scope of authorities. In this sense, the GDPR represents the first extraterritorial instrument of data protection, reflecting the EU's normative presumption that refuses to accept privacy as something limited to its political boundaries. In a few years, the GDPR revealed itself as a blueprint for other regulators and an influential channel for the global spread of transparent and coherent corporate best practices for the digital market. Still, the literature on regulatory convergence lacked a comprehensive explanation of the means by which this diffusion occurs. Based on a critical analysis of Anu Bradford's theory, this article has evaluated the explanatory power of the Brussels Effect with respect to the spread of GDPR data privacy standards. It presents original contribution enhancing Bradford's Brussels Effect in providing new evidence of the causal mechanisms which explain how EU self-regulation (aimed at enhancing the protection of individuals' privacy) has ultimately been able to transform corporate and national data protection standards beyond the EU. Moreover, it contributes to existing scholarship on the regulatory convergence of privacy laws by demystifying established convictions about the technical functioning of the data, their processing, and localization – like in the case of Drezner, and the previous analysis carried out by Bradford – and showing how they operate today, what challenges they pose for governments, companies, and other organizations as well.

The article shed light on the scale and degree of regulatory convergence. The years 2016 and 2018, both meaningful in the development of the GDPR, display a proactive response by many jurisdictions beyond the EU, rapidly aligning with its newly enforced requirements. The evidence show an increasing convergence towards European elements of data protection compared to Graham Greenleaf's study in 2012. Remarkably, higher convergence was found in countries more involved in the European digital market, endorsing Bradford's theory of a market-driven diffusion of data privacy norms.

In key respects, this analysis reinforces Bradford's theory but also refines it. The large, evenly regulated Single Market represents an important source of revenue for many companies operating online, especially multinational tech giants. The GDPR has come to be considered a model in other national jurisdictions despite the evident burdens that it places on data-driven markets. In fact, it was designed to be an easily exportable template for data protection. The quality of the provisions mostly derives from the EU's strong regulatory capacity in the matters of data protection guaranteed, among other things, by the existence of specialized auditing and supervisory bodies in this field.

A further reason that may have facilitated the diffusion of the law is the pressing demands by the EU citizens for more online security. On the other hand, companies may find it desirable for efficiency, competitiveness, and because a single set of norms exempt them from dealing with diversified compliance procedures and conflicting regulations. Mark Zuckerberg, Apple CEO Tim Cook, and Microsoft CEO Satya Nadella all endorsed the enforcement of a federal law for data protection on the model of the EU GDPR, whereas they opposed the idea of another patchwork of state laws (Schulze, 2019).

Finally, this article also contributes to refining and qualifying Bradford's original theory. Personal information does not constitute a completely inelastic target. At the same time, in less than 10 years, IT technologies changed to the extent that previous issues of non-divisibility have been overcome. However, new technical and economic constraints took over. Under article 25 of GDPR, services and products must be integrated with instruments of data protection by default. Moreover, ignoring new measures of data protection could prove a self-defeating business model and give a competitive edge to companies that base their strategy on protecting privacy. As an example, Facebook withdrew from the anti-CCPA campaign; Google, Uber, and Amazon joined indirectly through the mediation of lobbying groups like CalChamber and TechNet, probably for not being associated with an anti-privacy right campaign (Fang, 2018; Room, 2019). Eventually, forced to align with the GDPR, Big Tech Giants have contributed to the diffusion of similar business practices forcing smaller companies to align with the same standard if they want to have access to their platforms.

In conclusion, there is considerable evidence that the EU has had an important role in setting the standards for the current global data protection regime through a process that reflects the Brussels Effect. This research does not exclude other possible channels of diffusion of the EU standards, nor the valuable contribution of other jurisdictions to this legal field. Rather the purpose has been to analyze and explain the process and mechanisms of global regulatory convergence. In doing so, the analytical framework employed in this research, the Brussels Effect theory, has proven valuable for understanding the processes and mechanisms which result in global regulatory convergence in the field of data protection. In particular, it explains how the GDPR functions as a form of market regulation able to leverage the economic importance of the Single Market to induce both compliance and regulatory convergence.

Bibliography

Amazon. (n.d.a). *Alexa Privacy Hub*. November 24, 2021. https://www.amazon.com/Alexa-Privacy-Hub/b?ie=UTF8&node=19149155011.

Amazon. (n.d.b). *Alexa, Dispositivi Echo e la tua privacy*. Retrieved November 29, 2021. https://www.amazon.it/gp/help/customer/display.html?nodeId=GVP69FUJ48X9DK8V.

Apple. (n.d.a). *Privacy Governance*. Retrieved February 21, 2022. https://www.apple.com/legal/privacy/en-ww/governance/.

Apple. (n.d.b). *Privacy Policy*. Retrieved February 21, 2022. https://www.apple.com/legal/privacy/en-ww/.

Arnoldussen, T. (2019). The role of national problems in European air quality regulation: the process of amplification. *Int Environ Agreements, 19*, 207–224. https://doi.org/10.1007/s10784-019-09429-8.

Beach, D. (2016). It's all about mechanisms – what process-tracing case studies should be tracing.*New Political Economy, 21*(5), 463-472. https://doi.org/10.1080/13563467.2015.1134466.

Bennet, C. J. (2018). The European General Data Protection Regulation: An Instrument For The Globalization Of Privacy Standards? *Information Polity, 23*(2), 239-246. doi:10.3233/ip-180002.

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review, 107*(1), 1-68. https://ssrn.com/abstract=2770634.

Bradford, A. (2015). Exporting Standards: The Externalization Of The EU's Regulatory Power Via Markets. *International Review Of Law And Economics, 42*, 158-173. doi:10.1016/j.irle.2014.09.004.

Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard*International Data Privacy Law 6*(2), 77-78. https://doi.org/10.1093/idpl/ipw006.

Cataleta, A. (2019). GDPR, tra DPO e aziende (ancora) troppi problemi: ecco i punti critici. *Agenda Digitale.* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8983894.

Cavoukian, A., & Jolly, N. (2018). Embedding privacy and security to gain a competitive advantage.*Journal of Data Protection & Privacy, 1*(4), 400-409.

Chowdhry S., & Moes N. (2018, June 28). Trading Invisibles: Exposure Of Countries To GDPR. *Bruegel*. https://www.bruegel.org/2018/06/trading-invisibles-exposure-of-countries-to-gdpr/.

CNIL. (2022). *Cookies: la CNIL sanctionne GOOGLE à hauteur de 150 millions d'euros* . https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros.

Coffee, J. C. Jr. (1987). The Future of Corporate Federalism: State Competition and the New Trend Toward De Facto Federal Minimum Standards, *8 Cardozo L. Rev, 759*, 761–763.

ComRes. (2015). Digital Consumer Survey. *ETNO*. https://etno.eu/datas/publications/other/ComRes_ETNO_Final%20Report_LATEST%20FOR%20PUBLICATION.pdf.

Crews, C. W. (2001). One Internet Is Not Enough. *Techknowledge,* (3). https://www.cato.org/techknowledge/one-internet-not-enough.

Damro, C. (2012). Market power Europe. *Journal of European Public Policy, 19*(5), 682-699. https://doi.org/10.1080/13501763.2011.646779.

DLA Piper. (2022). "Data Protection Laws of the World". *DLA Piper.* Retrieved April 3, 2022 from https://www.dlapiperdataprotection.com/index.html.

Doig, J. M. (2016). *Impact of online privacy concerns and brand reputation on consumer willingness to provide personal information*. Queensland University of Technology. https://eprints.qut.edu.au/91648/.

Drezner, D. W. (2008). *All Politics Is Global: Explaining International Regulatory Regimes*. Princeton University Press.

Enforcement Tracker. (n.d.). *GDPR Enforcement Tracker", Enforcement Tracker*. Retrieved February 8, 2022. https://www.enforcementtracker.com/.

ENISA. (2019). *EDPS-ENISA Conference: Towards assessing the risk in personal data breaches* . https://www.enisa.europa.eu/events/edps-enisa-conference/edps-enisa-data-breaches-conference-notes

Eumonitor. (n.d.). *Decision-Making Procedures In The European Union*. Retrieved November 29, 2021. https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vg9tssega1vj.

European Commission. (n.d.a). *International Trade In Services*. Retrieved November 28, 2021. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=International_trade_in_services#Main_trading_partners.

European Commission. (n.d.b). *EU funding supporting the implementation of the GDPR*. Retrieved 29 November 2021. https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-

implementation-gdpr_en#earlier-activities.

European Parliament. (n.d.). *General Data Protection Regulation shows results, but work needs to continue*. Retrieved July 24, 2021. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449.

European Parliament. (n.d.). *Sources And Scope Of European Union Law*", Retrieved November 29, 2021. https://www.europarl.europa.eu/factsheets/en/sheet/6/sources-and-scope-of-european-union-law.

European Parliament. (2021). *The European Union And Its Trade Partners – Fact Sheets On The European Union*. https://www.europarl.europa.eu/ftu/pdf/en/FTU_5.2.1.pdf.

European Union. (1995). Directive 95/46/EC of the European Parliament and of the Council.*Official Journal of the European Communities, L 281*(31). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5.

European Union. (2000). Charter of Fundamental Rights of the European Union.*Official Journal of the European Communities, C 364*(1). https://www.europarl.europa.eu/charter/pdf/text_en.pdf

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR).*Official Journal of the European Union, 32*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679.

European Union Employment Advisor. (2020). *How Many Employees Does The European Commission Have?*. https://euemployment.eu/european-commission-employee-number/.

Facebook. (2019). *Facebook Reports Third Quarter 2019 Results*. Retrieved October 30, 2021. https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Third-Quarter-2019-Results/default.aspx.

Fang, L. (2018, June 26). Google and Facebook are quietly fighting California's privacy rights initiative, emails reveal. *The Intercept*. https://theintercept.com/2018/06/26/google-and-facebook-are-quietly-fighting-californias-privacy-rights-initiative-emails-reveal/

Fazlioglu, M. (2018). *How DPA Budget And Staffing Levels Mirror National Differences In GDP And Population*. The International Association of Privacy Professionals (IAPP). https://www.politico.eu/wp-content/uploads/2018/01/DPA-Budget-and-Staffing-Whitepaper.pdf.

Gal M., & Aviv, O. (2020). The Competitive Effects of the GDPR. *Journal of Competition Law and Economics*, 1-37. https://ssrn.com/abstract=3548444.

General Secretariat of the Council of the European Union. (2016). *Written Procedure*. http://www.europarl.europa.eu/cmsdata/99614/Procedure_ecrite_GDPR_EN.docx.

Gerrits, A. (2009). Normative Power Europe in a Changing World: A Discussion.*Netherlands Institute of International Relations Clingendael* (5). https://www.clingendael.org/sites/default/files/2016-02/20091200_cesp_paper_gerrits.pdf.

Gibbs, S. (2017, May 16). Facebook facing privacy actions across Europe as France fines firm €150k.*The Guardian*https://www.theguardian.com/technology/2017/may/16/facebook-facing-privacy-actions-across-europe-as-france-fines-firm-150k.

Google. (n.d.a). *Privacy Policy*. Retrieved February 21, 2022. https://policies.google.com/privacy?hl=en-US.

Google. (n.d.b). *Terms of Service*. Retrieved February 24, 2022- https://policies.google.com/terms/archive?hl=en-US.

Google. (2015). *Indexing HTTPS pages by default*. https://security.googleblog.com/2015/12/indexing-https-pages-by-default.html.

Gornitzka Å., & Sverdrup U. (2010). Access Of Experts: Information And EU Decision-Making. *West European Politics, 34*(1), 48-70. doi:10.1080/01402382.2011.523544.

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. *International Data Privacy Law, 2*(2), 68– 92. https://doi.org/10.1093/idpl/ips006.

Greenleaf, G. (2018). Global Convergence of Data Privacy Standards and Laws: Speaking Notes for the European Commission Events on the Launch of the General Data Protection Regulation (GDPR) in Brussels & New Delhi, 25 May 2018). *UNSW Law Research Paper*, (18-56), 1-8. https://ssrn.com/abstract=3184548.

Greenleaf, G., & Cottier, B. (2020). 2020 Ends a Decade Of 62 New Data Privacy Laws. *163 Privacy Laws & Business International Report, 24-26*. https://ssrn.com/abstract=3572611.

Guasch, J. L., & Hahn, R. W. (1999). The Costs and Benefits of Regulation: Implications for Developing Countries. *The World Bank Research Observer, 14*(1), 137-158. https://www.jstor.org/stable/3986542.

Hern, A. (2018, April 19). Facebook moves 1.5bn users out of reach of new European privacy law. *The Guardian*. https://www.theguardian.com/technology/2018/apr/19/facebook-moves-15bn-users-out-of-reach-of-new-european-privacy-law.

Hooghe, L. (2011). Images Of Europe: How Commission Officials Conceive Their Institution's Role. *JCMS: Journal Of Common Market Studies, 50*(1), 87-111. doi:10.1111/j.1468-5965.2011.02210.x.

Houser, K. A., & Voss, W. G. (2018). GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? [Working Paper] *25 Rich. J. L. & Tech.,* (1), 1-70. http://dx.doi.org/10.2139/ssrn.3212210.

Ingram, D. (2018, April 19). Exclusive: Facebook to put 1.5 billion users out of reach of new EU privacy law. *Reuters*. https://www.reuters.com/article/us-facebook-privacy-eu-exclusive/exclusive-facebook-to-put-1-5-billion-users-out-of-reach-of-new-eu-privacy-law-idUSKBN1HQ00P

Jeanite, S. (2019). *Data Protection Laws: Following GDPR Enactment, US States Take Action*. Cyber News. https://cyber.whiteandwilliams.com/2019/03/data-protection-laws-following-gdpr-enactment-us-states-take-action/.

Jeong, S. (2018, April 11). Zuckerberg says Facebook will extend European data protections worldwide — kind of. *The Verge*. https://www.theverge.com/2018/4/11/17224492/zuckerberg-facebook-congress-gdpr-data-protection see also https://about.fb.com/news/2018/04/new-privacy-protections/.

Kassim H., et al. (2013). *The European Commission Of The Twenty-First Century*. Oxford University Press.

Kerr, C. (1983). *The Future of Industrial Societies: Convergence or Continuing Diversity?* Harvard University Press.

Kodde, C. (2016). Germany's 'Right to be forgotten' – between the freedom of expression and the right to informational self-determination. *International Review of Law, Computers & Technology, 30*(1-2), 17–31.

Massé, E. (2020). *Two Years Under The EU GDPR*. Access Now. https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf.

McQuinn, A., & Castro, D. (2019). The Costs of an Unnecessarily Stringent Federal Data Privacy Law. *Information Technology & Innovation Foundation*. https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law.

Menn, J. (2020, February 19). Exclusive: Google users in UK to lose EU data protection – sources. *Reuters*. https://www.reuters.com/article/us-google-privacy-eu-exclusive-idUSKBN20D2M3.

Microsoft. (n.d.). *Privacy at Microsoft*. Retrieved February 24, 2021. https://privacy.microsoft.com/en-us/

Mitchener, B. (2002, April 23). Rules, Regulations of Global Economy Are Increasingly Being Set in Brussels.*The Wall St. J*. https://www.wsj.com/articles/SB1019521240262845360.

Molnár-Gábor, F. (2018). Germany: a fair balance between scientific freedom and data subjects' rights?*Hum Genet, 137*(8), 619-626, doi:10.1007/s00439-018-1912-1.

Moravcsik, A. (2017, April 13). Europe Is Still a Superpower. *Foreign Policy*. https://foreignpolicy.com/2017/04/13/europe-is-still-a-superpower/.

Ng, W. (2019). Changing Global Dynamics And International Competition Law: Considering China'S Potential Impact. *European Journal Of International Law, 30*(4), 1409-1430. doi:10.1093/ejil/chz066.

Office of the United States Trade Representative. (n.d.). *European Union*. Retrieved November 28, 2021. https://ustr.gov/countries-regions/uropa-middle-east/uropa/uropan-union#:~:text=Services%20exports%20were%20%24200%20billion,was%20%2454%20billion%20in%202019.&text=U.S.%20goods%20exports%20to%20the,up%2053%20percent%20from%202009.

Pagallo, U. (2016). The Impact of Domestic Robots on Privacy and Data Protection, and the Troubles with Legal Regulation by Design. *Data Protection on the Move, 403*, 387-410. doi: https://doi.org/10.1007/978-94-017-7376-8_14.

PwC. (2017). *GDPR Compliance Top Data Protection Priority for 92% of US Organizations in 2017, According to PwC Survey*. https://www.pwc.com/us/en/press-releases/2017/pwc-gdprcompliance-press-release.html.

Regulatory Imperialism. (2007, October 26). *The Wall St. J.* https://www.wsj.com/articles/SB119334720539572002.

Romm, T. (2019, February 8). 'There's going to be a fight here to weaken it': Inside the lobbying war over California's landmark privacy law. *The Washington Post*. https://www.washingtonpost.com/technology/2019/02/08/theres-going-be-fight-here-weaken-it-inside-lobbying-war-over-californias-landmark-privacy-law/

Schulze, E. (2019). Mark Zuckerberg says he wants stricter European-style privacy laws — but some experts are questioning his motives. *CNBC*. https://www.cnbc.com/2019/04/01/facebook-ceo-zuckerbergs-call-for-gdpr-privacy-laws-raises-questions.html

Schwartz, P. M. (2013). The EU-U.S. privacy collision: a turn to institutions and procedures.*Harvard Law Review, 126*(7), 1966. https://ssrn.com/abstract=2290261.

Statcounter. (n.d.a). *Browser Market Share Worldwide – Oct 2020 – Oct 2021* . Retrieved November 29, 2021. https://gs.statcounter.com/browser-market-share.

Statcounter. (n.d.b). *Search Engine Market Share Worldwide – Oct 2020 – Oct 2021* . Retrieved November 29, 2021. https://gs.statcounter.com/search-engine-market-share.

Statista. (2020). *Staff of the European data protection authorities (DPAs) 2019, by country* . https://www.statista.com/statistics/1174494/data-protection-authorities-staff-eu/

Strzelecki A., & Rizun, M. (2020). Consumers' security and trust for online shopping after GDPR: examples from Poland and Ukraine. *Digital Policy, Regulation and Governance, 22*(4), 289-305.

https://www.emerald.com/insight/content/doi/10.1108/DPRG-06-2019-0044/full/html.

Swire, P. (2013). The Second Wave Of Global Privacy Protection: Symposium Introduction. *74 Ohio State Law Journal, 74*(6), 841-853. https://ssrn.com/abstract=2404261.

The Administrative Council for Economic Defense (CADE). (2019). *BRICS In The Digital Economy: Competition Policy In Practice*. http://en.fas.gov.ru/documents/documentdetails.html?id=15348.

The Economist. (2021, April 24). The Brussels Effect: The EU Wants To Become The World'S Super-Regulator In AI. https://www.economist.com/europe/2021/04/24/the-eu-wants-to-become-the-worlds-super-regulator-in-ai.

Trading Economics. (2021a). *China GDP per capita PPP*. Retrieved December 18, 2021. https://tradingeconomics.com/china/gdp-per-capita-ppp.

Trading Economics. (2021b). *United States GDP Per Capita PPP*. Retrieved November 28, 2021. https://tradingeconomics.com/united-states/gdp-per-capita-ppp#:~:text=GDP%20per%20capita%20PPP%20in,of%2039831.59%20USD%20in%201991.

UNCTAD. (n.d.). *Data Protection and Privacy Legislation Worldwide*. Retrieved February 21, 2022. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

Vogel, D. (1995). *Trading Up*. Harvard University Press.

World Bank. (n.d.). *GDP (Current US$) – United States*. Retrieved November 28, 2021. https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=US.

WorldLII. (2022). "National Data Privacy Legislation". Retrieved April 2, 2022. http://www.worldlii.org/int/other/NDPrivLegis.

Wurzel, R. K. W. (2006). *Environmental Policy-Making In Britain, Germany And The European Union*. Manchester University Press.

Young, A. R. (2015). The European Union As A Global Regulator? Context And Comparison.*Journal Of European Public Policy, 22*(9), 1233-1252. doi:10.1080/13501763.2015.1046902.

Zhao, W. (2018, February 1). *About the Companies' Personal Information Protection Compliance Rules Based on the Personal Information Security Specification*. Weixin. https://mp.weixin.qq.com/s?__biz=MzIxODM0NDU4MQ==&mid=2247484784&idx=1&sn=6c56a88d51f5197ee712e8e22af72027&chksm=97eab89aa09d318c7258c3d7873ffde97fd1c1569d9769758c47f78430c5d7c46f9667dbd8e1&scene=21#wechat_redirect.

Appendix

Figure 1: Proportion of new laws vs existing laws by decade. Figure 2: Number of new national data protection laws by year

Table 1: Indicators of externalization of European elements of privacy in non-EU jurisdictions

JurisdictionYear of publicationRegion1234567891011Total Costa Rica2016Latin America□□□□□□□□7Indonesia2016Asia□□□□□5Mexico2016Latin America□□□□□□□□□□10Ukraine2016Europe□□□□□□□□□□10Bermuda2016Caribbean□□□□□□□□□□10Indonesia2016Asia□□□□□□□7Qatar2016 Middle East□□□□□□□7São Tomé and Principe2016Africa□□□□□□□□□□10Turkey2016Europe□□□□□□□□□□10Guernsey2017Europe□□□□□□□□□□11Kazakhstan2017Central Asia□□□□□□6Kyrgyzstan2017Central Asia□□□□□□□8Mauritius2017Africa□□□□□□□□□□11Moldova20

17Europe□□□□□□□□□□□□11Montenegro2017Europe□□□□□□□□□□□10Peru2017Latin America□□□□□□□□□8San Marino2017Europe□□□□□□□□□□□□11Cayman Islands2017Caribbean□□□□□□□□□10Niger2017Africa□□□□□□□□□8PRC2017Asia□□□□□□□6Turkmenistan2017Central Asia□□□□□□□□7Argentina2018Latin America□□□□□□□□□□□□11Canada2018North America□□□□□□□□□□9Chile2018Latin America□□□□□□□□□□9India2018Asia□□□□□□□□□□□10Indonesia2018Asia□□□□□□□□□□□□11Isle of Man2018Europe□□□□□□□□□□□□11Israel2018Middle East□□□□□□□□7Jersey2018Europe□□□□□□□□□□□□11Liechtenstein2018Europe□□□□□□□□□□□□11New Zealand2018Australasia□□□□□□□□7Serbia2018Europe□□□□□□□□□□9South Korea2018Asia□□□□□□□□□□□10Uruguay2018Latin America□□□□□□□□□□□□11Algeria2018Africa□□□□□□□□□□9Bahrain2018Middle East□□□□□□□□□□□□11Bhutan2018Asia□□□□□□□6Botswana2018Africa□□□□□□□□□□9Brazil2018Latin America□□□□□□□□□□□□11Lebanon2018Middle East□□□□□□□6St Kitts & Nevis2018Caribbean□□□□□□□□7Tajikistan2018CentralAsia□□□□□□□□7Thailand2019Asia□□□□□□□□□□□10Zimbabwe2019Africa□□□□□□□□□□□□11Barbados2019Caribbean□□□□□□□□□□□□11Kenya2019Africa□□□□□□□□□□10Nigeria2019Africa□□□□□□□□7Panama2019Latin America□□□□□□□□□8Republic of Congo2019Africa□□□□□□□□□□□□11Uganda2019Africa□□□□□□□□□□□□10Uzbekistan2019Central Asia□□□□□□□□□□9PRC2020Asia□□□□□□□□□□□□10Dubai DIFC2020Middle East□□□□□□□□□□□□11Nigeria2020Africa□□□□□□□□□□□□11Egypt2020Africa□□□□□□□□□□9Jamaica2020Caribbean□□□□□□□□□□□10North Macedonia2020Europe□□□□□□□□□□□□11Togo2020Africa□□□□□□□□□□□□1042555454575454513242405 35

The acts are displayed in chronological order, divided into two sub-categories differentiated by the colour. Those highlighted in red are "second-generation" laws, meaning that they refer to a state that already had a previous regulation but which, over this timeframe, proposed a new bill or enacted a new version of it. Of the total documents issued between 2016 and 2020, those enacted by EU Member States were excluded, as they show compliance for obvious reasons of intra-EU regulatory harmonization. Besides these, further 7 legislations have been omitted because the acts were either not accessible or lacked a reliable source.