



City Research Online

City St George's, University of London

Citation: Fahey, E. (2025). Data protection and regulation of social media. In: Lucarelli, S. & Sperling, J. (Eds.), Handbook of European Union Governance. Political Science and Public Policy 2025. (pp. 143-155). Edward Elgar Publishing. ISBN 9781803925172 doi: 10.4337/9781803925189.00021

This is the accepted version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: <https://city-ref-test.eprints-hosting.org/id/eprint/35297/>

Link to published version: <https://doi.org/10.4337/9781803925189.00021>

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to [City Research Online policy](#).

Elaine Fahey is Professor of Law at the Institute for the Study of European Law (ISEL), the City Law School, University of London (United Kingdom).

Chapter 11_Data Protection

GDPR	General Data Protection Regulation
DMA	Digital Markets Act
DGA	Data Governance Act
TTCs	Trade and Technology Councils
OOS	one-stop-shop
DPA	data protection agency
LSA	Lead Supervisory Authority
CSA	Concerned Supervisory Authority
EDPB	European Data Protection Board
IDPC	Irish Data Protection Commission
ICCL	Irish Council for Civil Liberties
VLOP	very online large platform
VLOSE	very large online search engine
DSA	Digital Services Act
AIA	Artificial Intelligence Act
AI	Artificial Intelligence

Common to all:

EC
ECSC
EEC
EU
NATO
OSCE
TEC
TEU
TFEU
UK
UN
US
WTO
EP

THE EU GOVERNANCE ROLE IN THE AREA OF DATA PROTECTION AND REGULATION OF SOCIAL MEDIA: THE INSTITUTIONALIZATION OF ‘BIG TECH’ REGULATION

Elaine Fahey

ABSTRACT

This chapter outlines how a whole swathe of highly significant EU regulation, from the Digital Markets Act and Digital Services Act to the Artificial Intelligence Act, forms a significant part of the new agenda on data. The post-General Data Protection Regulation era will radically change the face of Big Tech and how it engages with EU law. It will usher in a more directed era of EU law that protects consumers. Citizens have been protected through transnational law-making. It has been lauded by EU law-makers as the constitution of the digital age. But it has a distinctively specific set of subjects and objects in Big Tech, unlike or at least well beyond its previous law-making efforts. The EU has emerged as a regulatory juggernaut vis-à-vis Big Tech and has shown itself to be broad-ranging and beyond comprehensive, with a vast enforcement architecture. The rise of the force and reach of EU law in the quest for data protection has taken effect with considerable reach. The chapter examines the institutionalization of EU data governance law; the scope of EU law regulating Big Tech; the regulation of social media through enforceable remedies and bureaucracy; Big Tech qua Europeanists; and the ‘Brussels Effect’ of EU law for Big Tech.

Keywords: Big Tech; regulation; institutionalization; digital platforms; General Data Protection Regulation (GDPR); Digital Services Act (DSA); Digital Markets Act (DMA)

Digital platforms are now ‘repeat players’ in European Union (EU) law where they repeatedly and regularly litigate across jurisdictions to obtain results. Outside of courts, digital platforms are increasingly vociferous lobbyists, often seeking to influence EU

standards. Digital platforms are increasingly the subject and object of EU regulation as it seeks to constrain private power in the form of platforms. Data institutionalization can arguably be understood to be part of this global agenda, as the EU is driving the convergence of data protection laws and practices (Fahey 2022, 2023).

The EU's data protection law is a specific legal regime that is broadly understood to have had global reach and effects (European Commission 2017). Digital regulation arguably constitutes much more to the EU, as a constitutional evolution for the 21st century. The Europeanization of data protection has become a diplomatic as much as an enormous legal victory for the EU but it has also generated importantly the transition of Big Tech companies into 'Europeanists': they proclaim regularly the need for EU law standards to be adopted elsewhere in the absence of regulation and standards (Lynskey 2016). The EU fundamentally diverges from and even abnegates views that the internet and digital platforms are ungovernable, operate lawlessly or that Big Tech operates without regulation – which as a transnational organization of its size is highly significant (Suzor 2019).

The EU has the advantage of constituting the first mover globally, and also the first mover with the highest standards. Anu Bradford (2020) describes how EU regulations impact standards around the world through the process of unilateral regulatory globalization. It is most influential with respect to the digital economy in relation to the acceptance of leading social media tech giants in the US of EU law principles, from hate speech to the 2020 General Data Protection Regulation (GDPR), and it dominates EU law scholarship as much as EU official thinking on how to see the regulation possibilities and successes as to Big Tech. Yet it is more than a conceptual take or framing of EU law and policy: it is a largely descriptive claim on how the internet and Big Tech engages with EU law.

European data protection law rests on the assumption that individuals should have control of their personal data. This control is often labelled as “informational self-determination” (Thouvenin 2021: §1; Kuner et al. 2020: 157) which is an underlying rationale of the fundamental right to the protection of personal data as enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (European Commission 2012). It is understood to relate to the individuals' right to determine which information about themselves will be disclosed, to whom, and for which purpose (de Terwangne 2012: 112; Rouvroy and Pouillet 2009; Schwartz 1989). It differs historically to a degree from US self-management of data privacy, which is not a form of concept applicable to EU law (Solove 2013). This distinctive turn, backed up by a broad bureaucratization of rights through an architecture of decentralised enforcement with oversight, has generated one of the most

important knowledge self-management divides culturally and globally. In this sense, it is an important question of transnational regulation and EU efforts to evolve the global debate on terms consistent with existing EU law.

The right to the protection of personal data, enshrined in Article 16 of the Treaty on the Functioning of the European Union (TFEU: 2012) and Article 8 of the EU Charter of Fundamental Rights (European Commission 2012), is primary EU law and subject to a vast enforcement regime at the national and EU levels. In each member state, there is a data protection authority (DPA) that supervises the application of the data protection law and handles complaints against its violations, and a vast range of procedures and remedies are applicable, as is outlined below in the second section. US shifts towards EU-based ideas, e.g., the American Law Institute's 'Principles of the Law, Data Privacy' (ALI) and adoption of the GDPR by several US states, entail a significant push towards European understandings of privacy and rights. Yet still there is no federal agency or federal privacy law (ALI 2020; Rouvroy and Pouillet 2009; Vogiatzoglou and Valcke 2022; Council of Europe et al. 2018; Hoofnagle et al. 2019; Hijmans 2016; Bieker 2022; De Hert and Gutwirth 2009).

The chapter proceeds from the basis of an EU law and global governance account of the evolution of data protection as to Big Tech in the EU (Fahey 2022). It further proceeds on the basis that Big Tech in the EU operates businesses globally, i.e., as transnational entities, and it purports to show descriptively how in some instances EU law operates with global effects or as a medium for Big Tech to deploy as erstwhile Europeanists. The chapter refers to 'Big Tech' and EU law throughout to denote the EU's regulation of social media. It considers the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) predominantly, the Digital Services Act (DSA) (Regulation (EU) 2022/2065) and Digital Markets Act (DMA) (Regulation (EU) 2022/1925) less so (European Parliament and the Council 2016, 2022a, and 2022b). It then proceeds as follows: it outlines the institutionalization of EU data governance law; the regulation of social media through enforceable remedies and bureaucracy; and the scope of EU's laws regulating Big Tech that has generated an alphabet soup of regulation and governance. It then reflects upon Big Tech as Europeanist.

THE EMERGENCE OF THE EU AS AN AGENT OF THE INSTITUTIONALIZATION OF EU DATA GOVERNANCE LAW

The European Strategy for Data aims at creating a single market for data that will ensure Europe's global competitiveness and data sovereignty (European Commission, 2020). Common European data spaces are proposed in a variety of areas to harmonise rules on fair access to and use of data. The DMA is an iconic piece of EU law adopted in late 2022, alongside the Digital Service Act, as much as the Data Governance Act (for non-personal data) are key planks of the European Commission strategy, *Shaping Europe's Digital Future*. The DMA makes provision for a series of rules as to undertakings to be labelled as 'gatekeepers' on markets for digital services that constitute a critical gateway for business users to reach end users through so-called platform services. The EU Data Governance Act (DGA) (Regulation (EU) 2022/868) is a key pillar of the European strategy for data, the main objective of which is to make Europe a leader in the data economy by harnessing the potential of the ever-increasing amount of industrial data in order to benefit the European economy and society (European Parliament and the Council 2022c). DGA seeks to foster public sector information reuse, to create a supervisory framework for the provision of data sharing services, and to establish a framework for voluntary registration of entities which collect and process data made available for altruistic purposes. The Artificial Intelligence Act (AIA) (European Commission, 2021a), based upon conventional EU legal wisdom on the regulation of products and risk regulation, constitutes the world's first attempt at binding law-making globally as the world grapples with the highly risky era of Artificial Intelligence (AI)

The EU's data governance packages are iconic and far-reaching, largely through the EU's unique commitment to the 'institutionalization' of data (Fahey 2022). The EU's efforts on institutionalization have been argued to be usefully studied through data given that EU rules, actors and standards are considered internationally to be some of the highest global standards or at worst to set complex bars for international cooperation and international debates on data flows (see EPIC n.d.; Zuboff 2019). The EU's institutionalization practices are arguably hampered by other factors. For instance, adequacy decisions increasingly place indirectly complex constraints on trade negotiations (Fahey 2022: 5). I have argued nonetheless that institutionalization - the process of embedding concepts or norms within a governing organizational structure - is arguably the solution to most of the world's problems

but it is rarely scientifically developed (Fahey 2022: 1). This is evident in EU efforts on institutionalization in data transfer and data governance regimes under EU law covering topics ranging from data privacy and data transfers to cyber law and policy. A more traditional form of institutionalization - but not characteristic of transatlantic relations – is the Transatlantic Data Review Court established as one element of the recent EU-US Transatlantic Privacy Framework Agreement. The Court in an agreement appears to have been a precondition for the evolution of the EU-US Trade and Technology Councils (TTC), one of the foremost global initiatives on trade and technology (European Commission 2022b; see also European Commission 2023). Data institutionalization is evolving in EU external relations, with the potential to change the international landscape of data governance. In this regard, I argue that there is a very limited capacity for domestic Member States to evolve practices or policies; this is largely a strength of external relations law which enables the EU as a collection of often small states to have a voice in global governance. The bureaucratization of data governance by the EU is far-reaching and has had an impact because it has extensive agendas (e.g., cybersecurity or trade), is not limited to internal EU law, and has a significant external dimension.

EU GOVERNANCE OF SOCIAL MEDIA: THE REGULATION OF BIG TECH THROUGH ENFORCEABLE REMEDIES AND BUREAUCRACY IN THE GDPR

Organization, sanction and complaint

As outlined above, a key feature of EU data governance law is its use of EU institutionalization, whereby bureaucracy, institutions, and core EU architectures have been deployed with success to create a regime of unparalleled sophistication globally as to data protection. It constitutes a formidable architecture of GDPR supervision mechanisms, authorities, and procedures governing national operation. One of the most critical elements of EU law is its enforcement through the doctrines of direct effect and supremacy at national level (C-26/62 *Van Gend en Loos v Administratie der Belastingen*; C-6/64 *Costa v E.N.E.L (ECJ 1963)*). EU law derives its success through the effectiveness of EU law, which takes effect on account of these doctrines. A vast apparatus of provisions is provided for in the GDPR as to supervision mechanisms, authorities and procedures and, from a legal

perspective, constitutes one of the most significant practical forms of emphasis of the GDPR as to social media.¹ Article 77 GDPR provides that Data Subjects have the right to lodge complaints concerning the processing of their personal data with a DPA in the Member State in which they live or work, or the Member State in which the alleged infringement occurred. The DPA is required to keep the data subject informed on the progress and the outcome of the complaint. The Court of Justice of the European Union (CJEU) in Case C-132/21 *Budapesti Elektromos Művek* (CJEU 2023) held that the remedies in Articles 77(1), 78(1) and 79(1) GDPR could be exercised independently from one another, even when these remedies covered the same facts. The Court ruled that it was up to the Member States to ensure the consistent and homogeneous application of such GDPR provisions, but they also had to provide fundamental rights safeguards.

Pursuant to Article 78-79 GDPR data subjects have the right to an effective judicial remedy against decisions of a DPA concerning them, any failure by a DPA to deal with or respond to a complaint within three months, and any unlawful processing of their personal data by a controller or processor. According to Article 78(3) and 79(2) GDPR, proceedings against a DPA or public authority must be brought in the Member State in which the DPA is established. Proceedings against a controller or processor may be brought in the Member State in which the controller or processor has an establishment or the Member State in which the data subject resides.

A not-for-profit body, organization or association, whose statutory objectives are in the public interest and which is active in the field of the protection of data subjects' rights and freedoms, may lodge a complaint to a DPA on behalf of a data subject or exercise the right to judicial remedy and the right to seek compensation on behalf of data subjects on account of Article 80 GDPR. Under national law, Member States may designate a body to lodge complaints on behalf of data subjects, without being mandated by those data subjects. The CJEU held recently that under Article 80(2) GDPR, national legislations may allow consumer protection associations to bring legal proceedings for GDPR violations. That is so even when they have not been specifically authorised for this purpose, and is independent of the rights of data subjects. As a result, some of the leading case law relates to social media operating

¹ A massive number of national cases taken before national authorities are beyond the scope of this chapter but are well documented by the NOYB non-Governmental organization. See NOYB's website at <https://noyb.eu/en/project/cases>; see also GDPRHub website at https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub.

across the EU (e.g., *C-319/20 Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände* (CJEU 2022b)). This constitutes an important protection under EU law within the umbrella of the one-stop-shop (OOS) mechanism and thus accommodates at a transnational level the complexity of engaging with Big Tech 'globalness'. A not-for-profit body, organization or association whose statutory objectives are in the public interest and which is active in the field of the protection of data subjects' rights and freedoms may lodge a complaint to a DPA on behalf of a data subject or exercise the right to judicial remedy and the right to seek compensation on behalf of data subjects on account of Article 80 GDPR.

It is important to state that citizens are protected most through effective rights and enforceable action, and the GDPR has a key system of protection as follows. First, a data subject who has suffered harm as a result of the unlawful processing of his or her personal data has the right to receive compensation from the controller or processor for the harm suffered pursuant to Article 82(1)-(2), (4) GDPR. Second, any controller involved in the processing is liable for the harm caused, and a processor is liable for the harm caused by any of its (or its sub-processor's) processing activities that are not in compliance with its obligations under the GDPR or are in breach of the controller's instructions. Third, each controller or processor will be held liable for the entirety of the harm caused, if they are involved in the same processing and responsible for that harm. to ensure effective compensation.

Each DPA shall ensure that it imposes sanctions and administrative fines in a manner that is effective, proportionate, and dissuasive. Where a Member State's legal system does not provide for administrative fines, fines may be initiated by the DPA and imposed by the national courts. According to Article 83(5)-(6) GDPR the maximum fine that can be imposed for serious infringements of the GDPR is the greater of €20 million or four percent of an undertaking's worldwide turnover for the last financial year.

Member States set their own rules on penalties applicable to infringements of the GDPR, in particular those infringements that are not subject to administrative fines according to Article 84 GDPR. Member States may also provide their own rules on criminal sanctions for infringement of the GDPR. In 2023, Facebook owner Meta was fined €1.2bn by Ireland's Data Protection Commissioner after a decision of the EDPB, which ordered Meta to suspend the transfer of user data from the EU to the US, in one of the most significant developments of the GDPR enforcement architecture to date (DPC 2023). However, much conflict between a national authority (the Irish DPC) and the EU regulatory on the applicable fine is an

important outcome in the run up to it. This leads to a consideration of the place of the OSS within the architecture and the relationship between the national and transnational here.

THE EU'S ONE-STOP-SHOP....IN DUBLIN

The GDPR's one-stop-shop system is one key way in which Big Tech has been institutionalised into EU law and has found the might of their transnational influence tamed. Under the so-called one-stop-shop mechanism (Art. 60 GDPR), the Lead Supervisory Authority (LSA) is the authority in charge of leading the cooperation process through sharing relevant information with the Concerned Supervisory Authority (CSA), carrying out the investigations, preparing the draft decision relating to the case, and cooperating with the other CSAs to reach consensus on this draft decision (EDPB 2021). It has had a dramatic impact upon one jurisdiction, namely Ireland, with its authority hamstrung into adopting complex positions on Big Tech that appear the anthesis of its enforcement intentions.

When a LSA issues a draft decision, it consults the CSAs, which can express their disagreement. When none of the CSAs objects, the LSA may proceed to adopt the decision. In case at least one of the CSAs has expressed a relevant and reasoned objection (RRO), and if the LSA intends to follow the objection, it shall submit a revised draft decision to all the CSAs. The CSAs then have a period of two weeks (Art. 60 (5) GDPR) to express their RROs to the revised draft decision. However, if the LSA does not intend to follow the objection(s), since no consensus can be reached, the consistency mechanism is triggered and is obliged to refer the case to the European Data Protection Board (EDPB), which activates the EDPB's dispute resolution role (Art. 65(1)(a) GDPR). Within one month from the referral of the subject matter, the EDPB must adopt a decision by a two-thirds majority.

The OOS has operated in practice to privilege Dublin, Ireland as the lead enforcement entity of the GDPR given the high number of Big Tech companies headquartered. Consequently, the Irish Data Protection Commission (IDPC) has assumed much significance for Big Tech. Dublin has become the de facto and de jure European headquarters for much of global Big Tech because they are the beneficiaries of Ireland's low corporate tax rate and light touch regulatory regime generally- albeit still being within the EU. Under the GDPR, the IDPC has assumed significant responsibility for the enforcement of the GDPR in Europe and even globally. The activation of the OSS has entailed an outsized role for a very small authority within a regime and jurisdiction of lighter-touch regulation.

The Irish Council for Civil Liberties (ICCL), in a five-year review of the GDPR, has shown that there has been little substantial enforcement in EU-level cases (ICCL 2023). The EDPB register of final decisions reveals that most (63 percent) of the 160 enforcement measures by late 2022 were merely reprimands (ICCL 2023). It has shown how unlike any other country's enforcement authority, 67 percent of the IDPC's GDPR investigation decisions in EU cases were overruled by majority vote of its European counterparts at the EDPB, who demand tougher enforcement action. Moreover, the enforcement architecture of the GDPR has been argued to suffer chronic underinvestment, and while EEA data protection authorities' budgets are rising, 10 national DPAs still have budgets under €2 million (ICCL 2023). Still, Dublin demonstrates the fragility of the OOS. This raises the broader question of the place of Europe and the local in the regulation of Big Tech and the increasingly scope of Big Tech regulation, given the challenges of the institutionalization of data governance law.

THE EU AS A GLOBAL ACTOR: THE SCOPE OF EU LAWS REGULATING BIG TECH BEYOND THE GDPR

The EU efforts to create a regulatory regime defining the rights and responsibilities of those providing data and those using it has created an alphabet soup of regulation and governance. The EU's introduction of the DMA, in particular, represents an attempt to radically evolve the regulation of Big Tech at the supranational level (European Commission 2020a). It attempts in Article 3 to define gatekeepers as entities with a significant impact on the EU internal market that operate one or more important gateways to customers and enjoy an entrenched and durable position in its operations. It proposes to create a narrowly defined set of objective criteria for qualifying a large online platform as a so-called gatekeeper in order to tackle large systemic online platforms and institutionalise them as subjects and objects of EU law in a manner not previously achievable (Colombo 2021; European Parliament 2021a; European Commission 2020b).²

The DSA provides for four specifically key sets of rules on intermediary services, hosting services, online platform services, and very large online platform services. All online intermediaries offering their services in the EU would have to comply with the new rules,

² The Biden Administration, on the eve of the first EU-US Summit in 2021, described the DMA as anti-American, a sentiment that remains unchanged (Espinoza and Politi 2021).

including those established outside of the EU (European Commission 2020c: 1). The DSA turns online platforms into judge, jury, and executioner when it comes to removing online content (European Parliament 2020). The DSA also requires general risk assessments whereby tech companies will need to ask themselves whether their platforms will invite threats to democracy and how to mitigate those risks (European Parliament 2021a, 2021b, European Commission 2022a). It is, in short, a massive regulatory turn overall.

The DMA is an iconic piece of EU law adopted in late 2022, alongside the DSA. Both are key elements of the European Commission strategy Shaping Europe's Digital Future but were also claimed as the agenda of the European Parliament Internal Market Committee from 2014 to 2021 (European Commission 2020b; European Parliament 2020). The DMA makes provision for a series of rules for labelling undertakings as 'gatekeepers' on markets for digital services which constitute a critical gateway for business users to reach end users through so-called platform services.

A highly significant procedure then is the designation decision to indicate that an undertaking is a gatekeeper as a matter of law. The identified criteria for such a designation relate to quantitative measures such as turnover and active businesses users or alternatively to range of qualitative criteria. These actions are all undertaken by the European Commission, operating in a highly significant form of regulation activities. The key feature of the DMA as legislation is that it operates ex ante prohibitions and is a regulatory regime apart from EU competition law. There are significant powers accorded to the European Commission to fine gatekeepers where the relevant prohibitions are infringed pursuant to Article 3.8 thereof, with seven sets of criteria, quantitative and qualitative. The DSA is an important legislative intervention to evolve rules on online intermediation service providers. Its goal is to ensure a safe digital space for European consumers. The DSA purports to regulate online intermediaries—online platforms—and how they deal with illegal content online and to incorporate liability exemptions for online intermediaries existing in EU law already. The DSA makes provision for additional obligations for online marketplaces, very online large platforms (VLOPs), and very large online search engines (VLOSE). These designations, similar to those found in the DMA, are the subject of a designation procedure by the Commission and thereafter the subject of an assessment of risks. Notably, the enforcement of the DSA is a matter for the national authorities of the intermediary Member State. However, the Commission is the main enforcers for VLOPs. The first few months of 2023 were a key period in EU law, when the Commission would begin to adopt procedural rules for the conduct of proceedings under the DMA and DSA. In short, it constitutes a radical legalization

of Big Tech through this institutionalization but much remains to be seen. Perhaps unsurprisingly, Amazon, in a demonstration of the resources, capacity and interests of Big Tech, was one of the first to litigate its designation (T-367/23 *Amazon Services Europe v Commission*) before the EU's General Court in Summer 2023 (CJEU 2023).

EU LAW SHIFTS ON DISINFORMATION AND HATE SPEECH: FROM SOFT LAW TO HARD LAW, FRIEND TO FOE?

One of the greatest challenges posed by Big Tech relates to their overarching ambitions to *circumvent* professional journalism on the internet and change free speech for citizens- a major transnational problem (Zuboff 2019). Both corporations such as Google and Meta (previously Facebook) have inserted themselves between publishers and their populations, subjecting journalistic content to the same categories of equivalence that dominate surveillance capitalism's other landscapes. Others note Facebook's decision to standardise presentation of its News Feed content so that 'all news stories looked roughly the same as each other... whether they were investigations in the Washington Post, gossip in the New York Post or flat-out lies in the Denver Guardian, an entirely bogus newspaper...' (Zuboff 2019: 507; Thompson and Vogelstein 2018). Meta's CEO has stated in European Parliament hearings that Facebook should not regulate what is true or not, representing a philosophical ideal that all political speech should be permitted with a plurality of views being represented (Lischka 2019), a position indicative of an understanding of expression more in line with a US regulatory approach under the 1st Amendment to the US Constitution (Carrapico and Farrand 2021).

In the run up to the EU elections in May 2019, the Commission devised the code of practice on disinformation to address the spread of online disinformation and fake news (European Commission 2018a, 2018b, 2018c; Renda 2018; Bentzen 2017). It was not a binding law but instead a 'co-regulatory' instrument negotiated with major tech companies including Google, Facebook, Twitter, Microsoft and Mozilla in late 2018, along with advertisers and the advertising industry (European Commission 2018c). The EU sought to show that this is the first time industry agreed worldwide on a voluntary basis to self-regulatory standards to fight disinformation, showing transparency in political advertising to the closure of fake accounts and demonetization of purveyors of disinformation. A Code of

Practice on Disinformation was a first-of-its kind tool through which relevant players in the industry agreed in 2018 on self-regulatory standards to fight disinformation.

Its revision process was launched in June 2021 and, after the signature and presentation of the revised Code on 16 June 2022, the new Code was to become part of a broader regulatory framework, in combination with the legislation on Transparency and Targeting of Political Advertising and the Digital Services Act. An EU regulation, originally announced in December 2020 as part of the Commission's Democracy Action Plan, was intended to increase the transparency of political advertising and tackle the issue of foreign interference in electoral campaigns (European Commission 2021b; Killeen 2023). The regulation required more information about the actors financing advertisements, engagement, who it might have been targeted at and based on what data, and whether it has been suspended for violating any of the regulation's provisions (Pollicino and Bietti 2019; European Parliament 2022).

Under the Digital Services Act (DSA), platforms must mitigate against risks such as disinformation or election manipulation, cyber violence against women, or harms to minors online. These measures must be carefully balanced against restrictions of freedom of expression, and are subject to independent audits. The DSA is an extremely significant law for its political reach on content moderation- The law is seen as a global benchmark for social media platforms and tech platforms after years of a light-touch regime on how they manage the content on their websites and servers — everything from trolls and fake users to hate messages, misinformation and cyber bullying- as a supranational code (Goujard 2022). These developments underscore the multifaceted challenges of Big Tech for the citizen, the local (if one can term Member States in that way) and the transnational.

Big Tech. The Europeanists?

Big Tech ultimately portrays itself to be a 'Europeanist', where it now subscribes to significant amounts of EU law ostensibly and readily, e.g. GDPR, advocacy of EU law as a global standard or voluntary adoption of EU codes of hate speech (Bradford 2020). It has created an important global debate about European ideals and values (Bradford 2020). Others have shown how online content providers such as YouTube, for example, are carefully positioning themselves to users, clients, advertisers and policymakers, making strategic claims for what they do and do not do, and how their place in the information landscape

should be understood (Gillespie 2010). Yet the place of Big Tech as Europeanists, making the case for EU law to become the global standard for instance, sets the EU apart even further as to these claims. The GDPR aside, there are multiple EU data governance innovations of note. It is, in short, an extraordinary span of law making. Whether the stance of Big Tech as ‘Europeanists’ continues and its ultimate destination remains to be seen. Amazon has already instituted significant litigation against the implementation of the DSA and the Commission’s decision to designate it as a VLOP (Case T-367/23 *Amazon Services Europe v Commission*, pending). The GAFAM (Google, Apple, Facebook, Amazon and Microsoft) have subjected Europe to a barrage of litigation as subject and object of the litigation. Claims of ‘Europeanists’ could be more complex to discern going forward. Finally, this leads to the broader question of ‘after’ the Brussels Effect and Big Tech in EU law.

Bradford’s iconic EU Brussels Effect notably depicted the attempts of Big Tech to advocate EU law as a global standard, chiefly its GDPR (Bradford 2020). The extraordinary success of EU law where the EU acted as a first mover at the vanguard of data protection law making has seen dozens of jurisdictions globally seek to follow its lead or plan to do so. In the past, Big Tech has often been at the forefront of this development, at least optically, advocating for the use of EU law as global standards- or developing their own standards in the hope of self-regulation prevailing otherwise. However, it was a short moment in time. Yet just *after* the adoption of the GDPR, many Europeans quickly found themselves unable to access US websites, with overly zealous legal interpretations thereof applied in the US initially, particularly in US media outlets.

Conceptually, however, a transatlantic gap still exists between the EU and US, that is of consequence to Big Tech where no federal privacy legislation applies to EU citizens, nor is there any federal privacy agency- and it poses a global problem as to creating a single set of globally agreed upon standards. Yet once derided by US legislators, scholars and Big Tech, today the EU’s GDPR is lauded and mimicked globally in an increasing array of jurisdictions (Schwartz 2013). As adverted to above, it is the inspiration for the ALI set of guidelines on model privacy principles developed by US lawyers. Notable recent developments, such as a Transatlantic Data Privacy Agreement and Court and the Joint EU-US Declaration on the future of the internet or joint shared principles on AI (see White House 2023), indicate some significant levels of convergence, but are always against the backdrop of highly significant domestic divergences. Significant litigation ahead may see other legislation- beyond the GDPR- challenged by Big Tech in the EU courts and not the national courts, although not lacking any less complexity. The question remains as to where EU law resides going forward

for Big Tech. Meta has ominously warned of needing to leave the EU in the face of regulatory changes or prospective adverse rulings- will it carry those threats through in one of its richest markets? Or will the EU's mighty efforts to regulate global issues matter more?

CONCLUSION

This chapter has outlined how a whole swathe of highly significant EU regulation, from the DMA, DSA to AI Act and more, is under implementation and development, which forms part of a significant new agenda on data, post-GDPR. It also includes a range of regulation of non-personal data, for example the Data Act, that will radically change the face of Big Tech and how it engages with EU law. It has been lauded by EU law-makers as the constitution of the digital age. But it has a distinctively specific set of subjects and objects in Big Tech, unlike or at least well beyond its previous law-making efforts. The fast-moving pace of digital technology may also mean that the EU's first mover advantage is quickly outpaced, as developments in AI, like ChatGPT, indicate (Volpicelli 2023). The regulatory juggernaut of the EU as to Big Tech has shown itself to be broad-ranging and multifaceted to protect citizens, even in the face of Anti-American claims from the US Government. It remains to be seen if there is a continuation of Big Tech to proclaim themselves to be Europeanists and what lies after the Brussels Effect- and the extent of its organizational efforts to regulate the global beyond the GDPR and into the 'Alphabet Soup'.

* The author is grateful to Ivanka Karaivanova for the research assistance provided. The paper develops further the study Fahey, Elaine (2023), 'Comparative Law Research on the Personal Data Protection Law in Various Countries' KGRI Working Paper 2023 at <https://www.kgri.keio.ac.jp/working-paper/>

REFERENCES

- ALI (American Law Institute) (2020), *Principles of the Law: Data Privacy* (Philadelphia: The American Law Institute Press).
- Bentzen, Naja (2017), 'Understanding disinformation and fake news', *PE 599.408* (European Parliamentary Research Service) at [https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599408/EPRS_ATA\(2017\)599408_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599408/EPRS_ATA(2017)599408_EN.pdf)
- Bieker, Felix (2022), *The Right to Data Protection Individual and Structural Dimensions of Data Protection in EU Law* (Asser: Springer).
- Bradford, Anu (2020), *Brussels Effect: How the European Union rules the World* (Oxford: Oxford University Press).
- Carrapico, Helena and Benjamin Farrand (2021), 'When Trust Fades, Facebook Is No Longer a Friend: Shifting Privatization Dynamics in the Context of Cybersecurity as a Result of Disinformation, Populism and Political Uncertainty', *JCMS: Journal of Common Market Studies*, 59(5): 1160=76.
- European Commission (2012), 'Charter of Fundamental Rights of the European Union', *OJ C 326/391-407*, 26 October.
- ECJ (European Court of Justice) (1963), 'Case C-26/62 *Van Gend en Loos v Administratie der Belastingen*', ECLI:EU:C:1963:1.
- ECJ (European Court of Justice) (1964), 'Case C-6/64 *Costa v E.N.E.L*', ECLI:EU:C:1964:66.
- CJEU (Court of Justice of the European Union) (2023), 'Case C-132/21 *Budapesti Elektromos Művek*', ECLI:EU:C:2023:2.
- CJEU (Court of Justice of the European Union) (2022a), 'Case C-300/21 *UI v Österreichische Post AG*', ECLI:EU:C:2022:756.
- CJEU (Court of Justice of the European Union) (2021), 'Case C-645/19 *Facebook Ireland Ltd and Others v Gegevensbeschermingsautoriteit*', ECLI:EU:C:2021:483.
- CJEU (Court of Justice of the European Union) (2022b) 'Case C-319/20 *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände*', ECLI:EU:C:2022:32
- CJEU (Court of Justice of the European Union) (2023), 'Case T-367/23 *Amazon Services Europe v Commission*', ECLI:EU:T:2024:1

- Ibáñez Colomo, Pablo (2021), 'The Draft Digital Markets Act: A Legal and Institutional Analysis', 22 February at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3790276
- Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights (2018), *Handbook on European Data Protection Law: 2018 Edition* (Brussels: Publications Office of the European Union).
- De Hert, Paul and Serge Gutwirth (2009), 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in Serge Gutwirth, Yves Poullet, Paul Hert, Cécile de Terwangne, and Sjaak Nouwt (eds), *Reinventing Data Protection?* (London: Springer), pp. 3-44
- de Terwangne, Cécile (2012), 'Internet Privacy and the Right to Be Forgotten/Right to Oblivion', *Revista de Internet, Derecho y Política*, No. 13: 109-20.
- EPIC (n.d.), 'The US Urgently Needs a Data Protection Agency' at <https://epic.org/dpa/>.
- Espinoza, Javier and James Politi (2021), 'US warns EU against anti-American tech policy', *Financial Times*, 15 June at www.ft.com/content/2036d7e9-daa2-445d-8f88-6fcee745a259
- European Commission (2017), *Communication from the Commission to the European Parliament and the Council: Exchanging and Protecting Personal Data in a Globalised World*, COM(2017) 07 final, 10 January.
- European Commission (2018a), *Recommendation on Measures to Effectively tackle illegal content online*, COM(2018) 1177 final, 1 March.
- European Commission (2018b), *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Tackling online disinformation: a European Approach'*, COM(2018) 236 final, 26 April.
- European Commission (2018c), 'EU Code of Practice on Disinformation' at <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation>
- European Commission (2020a), *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, COM(2020) 842 final, 15 December.
- European Commission (2020b), *Communication from the Commission to The European Parliament, The Council, The European Economic and Social Committee and The*

- Committee of The Regions, 'Shaping Europe's digital future', COM (2020) 67 final, 19 February.*
- European Commission (2020c), *Commission Staff Working Document, Impact Assessment: Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, SWD(2020) 348 final, 15 December.
- European Commission (2021a), *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, 21 April.
- European Commission (2021b), *Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising*, COM(2021) 731 final, 25 November.
- European Commission (2022a), *The 2022 Code of Practice on Disinformation at* <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>
- European Commission (2022b), *European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework*, 25 March at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087
- European Commission (2023), *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, COM(2023) 4745 final, 10 July.
- EDPB (European Data Protection Board) (2021), *Article 65 FAQ at* https://edpb.europa.eu/system/files/2021-09/20201110_art65_faq_en.pdf
- European Parliament, Committee on the Internal Market and Consumer Protection (2020), *Draft Report with recommendations to the Commission on Digital Services Act: Improving the functioning of the Single Market*, Report A9-0181/2020 at https://www.europarl.europa.eu/doceo/document/A-9-2020-0181_EN.html
- European Parliament (2021a), 'Digital markets act', *Briefing PE 662 at* [www.europarl.europa.eu/RegData/etudes/BRIE/2021/662641/EPRS_BRI\(2021\)662641_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2021/662641/EPRS_BRI(2021)662641_EN.pdf)
- European Parliament (2021b), 'Digital services act', *Briefing PE 689.357 at* [www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI\(2021\)689357_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689357/EPRS_BRI(2021)689357_EN.pdf)

European Parliament (2022), *Report on foreign interference in all democratic processes in the European Union, including disinformation*, A9-0022/2022 at https://www.europarl.europa.eu/doceo/document/A-9-2022-0022_EN.html

European Parliament and the Council (2016), ‘Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)’, *OJ L* 119/1-88, 4 May.

European Parliament and the Council (2022a), ‘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)’, *OJ L* 277/1-102, 27 October.

European Parliament and the Council (2022b), ‘Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)/’, *OJ L* 265/1-66, 12 October.

European Parliament and the Council (2022c), ‘Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)’, *OJ L* 152/1-44, 3 June.

Fahey, Elaine (2022), *EU as a Global Digital Actor* (London: Hart Publishing).

Fahey, Elaine (2023), ‘Comparative Law Research on the Personal Data Protection Law in Various Countries’ KGRI Working Paper 2023 at <https://www.kgri.keio.ac.jp/working-paper/>

Goujard, Clothilde (2022), ‘WTF is DSA? What Europe’s new content moderation law means for the internet’, *Politico*, 27 October at <https://www.politico.eu/article/5-things-to-know-about-the-eu-content-moderation-law-digital-services-act/>

Gillespie, Tarleton (2010), ‘The politics of “platforms.”’, *New Media & Society*, 12(3): 347-64.

Hijmans, Hielke (2016), *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU* (London: Springer).

- Hoofnagle, Chris Jay, Bart van der Sloot, and Frederick Zuiderveen Borgesius (2019), 'The European Union general data protection regulation: what it is and what it means', *Information & Communications Technology Law*, 28(1): 65-98.
- ICCL (Irish Council for Civil Liberties) (2023), *5 years: GDPR's crisis point*, 31 May at <https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf>
- Killeen, Molly (2023), 'EU Parliament adopts position on political advertising regulation', *Euractiv*, 2 February at <https://www.euractiv.com/section/platforms/news/eu-parliament-adopts-position-on-political-advertising-regulation/>
- Kuner, Christopher, Lee A. Bugrave, Christopher Docksey, and Laura Drechsler (2020), *The EU General Data Protection Regulation (GDPR): A Commentary* (New York: Oxford University Press).
- Leerssen, Paddy, Jef Ausloos, Brahim Zarouali, Natali Helberger, and Claes H. de Vreese (2019), 'Platform Ad Archives: Promises and Pitfalls', *Internet Policy Review*, 8(4) at <https://doi.org/10.14763/2019.4.1421>
- Lischka, Juliane A. (2019), 'Strategic Communication as Discursive Institutional Work: A Critical Discourse Analysis of Mark Zuckerberg's Legitimacy Talk at the European Parliament', *International Journal of Strategic Communication*, 13(3): 197-213.
- Lynskey, Orla (2016), 'The Europeanisation of Data Protection Law', *Cambridge Yearbook of European Legal Studies*, 19: 1-35
- Pollicino, Oreste and Elettra Bietti (2019), 'Truth and Deception Across the Atlantic: A Roadmap of Disinformation in the US and Europe', *Italian Journal of Public Law*, 11(1): 43-85.
- Renda, Andrea (2018), 'The legal framework to address "fake news": possible policy actions at the EU level', *In-Depth Analysis*, PE 619.013 (European Parliamentary Research Service) at [https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA\(2018\)619013_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf)
- Richter, Andrei (2023), 'For Propaganda Without Disinformation: Draft EU Regulation on Political Advertising', *EJIL Talk!*, 24 February at <https://www.ejiltalk.org/21919-2/>
- Rouvroy, Antoinette and Yves Poullet (2009), 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth, Yves Poullet, Paul Hert, Cécile de Terwangne, and Sjaak Nouwt (eds), *Reinventing Data Protection?* (London: Springer), pp. 3-44

- Schwartz, Paul (1989), 'The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination', *The American Journal of Comparative Law*, 37(4): 675-701.
- Schwartz, Paul (2013), 'The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures', *Harvard Law Review*, 126(7): 1966-2009.
- Solove, Daniel (2013), 'Introduction: Privacy Self-Management and the Consent Dilemma', *Harvard Law Review*, 126(7): 1880-1903.
- Suzor, Nicolas P. (2019). *Lawless: The Secret Rules That Govern our Digital Lives* (Cambridge: Cambridge University Press).
- Thompson, Nicholas and Fred Vogelstein (2018), 'Inside the Two Years that shook Facebook and the World', *Wired*, 12 February at <https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell/>
- Thouvenin, Ilorent (2021), 'Informational Self-Determination: A Convincing Rationale for Data Protection Law?', *JIPITEC*, 12: 246-56.
- TFEU (2012), 'Treaty on the Functioning of the European Union, Consolidated Version' *OJ C 326/47- 360*, 26 October.
- Vogiatzoglou, Plixavra, and Peggy Valcke (2022), 'Two Decades of Article 8 CFR: A Critical Exploration of the Fundamental Right to Personal Data Protection in EU Law', in Eleni Kosta and Ronald Leenes with Irene Kamara (eds), *Research Handbook on EU Data Protection Law* (Cheltenham: Edward Elgar), pp. 11-49.
- Volpicelli, Gian (2023), 'ChatGPT broke the EU plan to regulate AI', *PoliticoPro*, 5 March at <https://subscriber.politicopro.com/article/2023/03/chatgpt-broke-the-eu-plan-to-regulate-ai-00085531>.
- White House (2023), 'U.S.-EU Joint Statement of the Trade and Technology Council', *Statements and Releases*, 31 May at <https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/31/u-s-eu-joint-statement-of-the-trade-and-technology-council-2/>
- Zuboff, Shoshana (2019), *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Profile Books).