3 The More the Merrier

A Dynamic Approach Learning From Prior Misgovernance in EU Data Protection Law

Indra Spiecker gen. Döhmann

1 Introduction[1]

Data protection law could be considered to be the core legal regime of internet and digitalisation research. After all, it arose as a completely new field of regulatory approach to a technological development unknown until then—automated data processing and automated decision-making. As such, it can be compared to other legal areas which also addressed new technological phenomena, for example atomic energy or genetic engineering law.

However, the question remains whether the original setting and content of data protection law is still in sync with today's approach to regulation of the consequences of the use of digital tools, services and the necessary data processing accompanying our increasingly digitalised world. Maybe, so the hypothesis in the following chapter, learning about ubiquitous computing, big data, cloud computing, high-speed volume processing or artificial intelligence has altered the approach on how to control data processing and automated decision-making, and so we find a new legal regime.

This hypothesis could easily be affirmed considering the rhetoric when, in 2018, the European General Data Protection Regulation (GDPR)[2] took effect and the prior Data Protection Directive (DPD)[3] gave way. "The new framework is ambitious, complex and strict"[4] and "radical",[5] it "replaces the archaic Data

1 Due to the character of the chapter as an overview, an extensive catalogue of literature has been avoided.

2 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

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

4 Warwick Ashford, 'D-Day for GDPR is 25 May 2018' [2016] ComputerWeekly <www.computerweekly.com/news/450295538/D-Day-for-GDPR-is-25-May-2018> accessed 21 May 2021.

5 Larry Downes, 'GDPR and the End of the Internet's Grand Bargain' [2018] Harvard Business Review <https://hbr.org/2018/04/gdpr-and-the-end-of-the-internets-grand-bargain> accessed 21 May 2021.

DOI: 10.4324/9781003283881-6

Protection Directive 95/46/EC"[6] and it "is set to force sweeping changes in everything from technology to advertising, and medicine to banking".[7] At the same time, the EU DPD in place until then was described as "no longer relevant to today's digital age".[8]

However, a closer look at the present regulatory regime of data protection law in comparison to its onset may reveal a more differentiated result in analysis and thus help to better understand the effects of global digitality. The present analysis concentrates on a European approach, looking in particular at the GDPR and to what extent it addresses new phenomena and whether it construes new instruments and new goals.

2 The Historical Approach to Data Protection Law—An Overview

2.1 Goals

Data protection law has addressed four major goals from its beginning:

Firstly, it discovered automated decision-making as a new subject for regulation. In the 1960s, in particular State administrations, but also private entities realized a growing need for new information in an increasingly complex world that called for new information technology and new information processing to master these challenges.[9] New production devices, credit and loan business models and marketing needs in the private sector as well as a demand for governance and planning in the administrative area called for more information and better use of existing information and thus for new ways of organising and structuring data.[10] As automatisation of data processing was intended to make

6 Mihaela Lica Butler, 'GDPR Goes into Effect in May 2018. Is Your Business Compliant?' [2018] Carmelon Digital Marketing <www.carmelon-digital.com/articles/gdpr-general-data-protection-regulation/> accessed 21 May 2021.

7 Alex Hern, 'What is GDPR and How Will It Affect You?' [2018] The Guardian <www.theguardian.com/technology/2018/may/21/what-is-gdpr-and-how-will-it-affect-you> accessed 21 May 2021.

8 Andrew Rossow, 'The Birth of GDPR: What Is It and What You Need to Know' [2018] Forbes <www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/> accessed 21 May 2021.

9 Spiros Simitis and others, in Spiros Simitis/Hornung/Spiecker (eds), *Kommentar Datenschutzrecht. DSGVO mit BDSG* (1st edn, 2019) Introduction para 6; Jürgen Kühling and Johannes Raab, in Jürgen Kühling and Benedikt Buchner (eds), *Datenschutz-Grundverordnung Kommentar* (1st edn, 2017) Introduction para 37; Alan F Westin, 'Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I—The Current Impact of Surveillance on Privacy' (1966) 66 Colum L Rev 1003, 1003; Spiros Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 U Pa L Rev 707, 709ff.

10 Simitis/Hornung/Spiecker (n 9) Introduction para 7ff; Martin Selmayr and Eugen Ehmann, in Martin Selmayr and Eugen Ehmann (eds), *Datenschutz-Grundverordnung Kommentar* (2nd edn, 2018) Introduction para 9; Spiros Simitis, 'Reviewing Privacy in an Information Society' (1987) 135 U Pa L Rev 707, 709ff.

data available for multiple purposes, it quickly became obvious that information was now devoid of context and thus devoid of control of the subject of the information.

Secondly, based on this understanding, availability of data and the technical ability to make use of it created an imbalance of power until then unknown.[11] Whoever has the tools to collect and use available data, may then make use of this information for influencing decisions. As a consequence, individuals could become objects of (potentially positively) private and administrative planning, governance and (potentially negatively) manipulation and control. Thus, the core of data protection is to regulate the informational power asymmetry.

Thirdly, data protection required the regulation of data processing and thus clear enforceable legal rules. Behind this is the understanding that the impact of data processing can be so burdensome on individuals and their legal and societal interests that only a legislative act could ensure proper protection.[12] Other tools, in particular self-regulation of, for example, the private information technology industry would not suffice.

Finally, it had become clear that the processing of data was not a single act restricted to certain areas of life. Rather, data protection needed to address all areas where information technology and thus automated data processing was taking place.[13] This required umbrella regulation binding every act of data processing.

2.2 Instruments

Pursuing these four goals, the first data protection regulatory regimes—in particular in Hessia in Germany in 1970 as the world's first data protection law, but also in the European DPD in 1995—included particular instruments to achieve them. Among the many issues one could potentially raise here, only two will be pointed out in particular:

Firstly, these early data protection legal regimes were viewed in the tradition of technology law, thus making use of established principles and structures of this field of law. Automated decision-making was considered to be a new technology with unknown consequences that needed regulation and control, similar to atomic energy, emissions or chemicals. One consequence of this model function of technology law resulted in data protection laws acting from

11 Cf Simitis/Hornung/Spiecker (n 9) Introduction para 22; Orla Lynskey, *The Foundations of EU Data Protection Law* (1st edn, 2016) 1; cf Lorna Stefanik, *Controlling Knowledge—Freedom of Information and Privacy Protection in a Networked World* (1st edn, 2011) 29; Walter Schmidt, 'Die bedrohte Entscheidungsfreiheit' (1974) 29 JuristenZeitung 241, 246.

12 Cf Simitis/Hornung/Spiecker (n 9) Introduction para 17; Selmayr and Ehmann (n 10) Introduction para 18, 21; Schmidt (n 11).

13 Simitis/Hornung/Spiecker (n 9) Introduction para 19.

a preventive standpoint. They followed the principle of precaution as known in technology law. Rather than setting up new rules for liability or duties of care to govern from a secondary law approach, they focused on regulating the processing of data at its origin on the primary level. Thus, the results of data processing, the decisions following from the access to and use of data, were not typically addressed.[14]

Secondly, concerns about the frequent use of automated decision-making arose first in regard to the availability of data and information technology in the hands of the State. The reason for this can be understood in the availability and the state of art of the information and communication technology itself: In the 1960s and 1970s, only very few players had a need and the resources to make use of existing data processing tools. One should also not forget that information technology was often pushed forward by secret services and other State actions. If states increased their power over citizens, so the conclusion was, it was a highly threatening situation for human rights and the democratic idea.

Therefore, data protection laws at first primarily addressed the balancing of public interests favouring State access to and use of data and individual rights guaranteeing individual freedom and autonomy. Consequently, early influencing decisions such as the census decision of the German Constitutional Court in 1983 concentrate on limiting the power of the State while ignoring potential power shifts towards private entities due to the use of information technology and data processing. Private use of these technologies was, overall, addressed less frequently and less intensely. In consequence, the rise of the internet in the 1990s and the rise of private actors in data processing including ubiquitous access to data processing services, hard- and software has often been neglected.

3 Reaction of Today's Data Protection Law to the Challenges of Global Digitality

When looking at these beginnings of data protection one could conclude that little has changed. All of the previously mentioned goals of data protection law are still valid, the GDPR is based on them, and it seems—to answer the general question of this book—that data protection may prove to be a stronghold in legal regimes where digitalisation has not changed the existing approach to regulation much. This would even seem consistent with the finding that data protection from its beginning addressed digitality. Thus, one could easily state that global digitality has surpassed data protection, and rightly so.

14 Simitis/Hornung/Spiecker (n 9) Introduction para 17; Kühling and Raab (n 9) Introduction para 38.

However, when looking more closely at the individual provisions of the GDPR as the successor to the previous DPD, we do find some activity in regard to the special effects of digitalisation. After all, the GDPR is a reaction to some experiences on the basis of prior data protection law, of its ineffectiveness and its minimal and contradicting enforcement.[15] One may also add that the GDPR now reflects a better understanding of the value and qualities of information, the economic effects of its characteristic as a so-called "common good", as well as the particular importance of the internet cumulating, for instance, in "winner-takes-all" markets.[16]

A reaction to the enforcement deficit can be identified in a number of norms of the GDPR. Also, some findings of economics (information as a public good; the network effects of information infrastructure and social platforms) have clearly been the foundation of some norms (e.g. in data portability, Art. 20 GDPR). Also, we observe a reaction to globalisation in the distribution of information and use of information technology, and thus the need to regulate beyond national borders (e.g. in the market principle of Art. 3 para. 2 GDPR as well as some decisions of the CJEU, such as *Google Spain*, 2014).[17]

Based on these few general remarks about early data protection law, the following analysis will look at the dominant present regulatory regime in data protection, the GDPR. When looking at individual regulatory goals and tools, the comparison to the prior regulatory regime will be undertaken.

3.1 Core Regulatory Goals

The recitals of the GDPR provide a number of goals. No. 2 explicitly states that

> the Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

Considering this vast amount of goals, one could declare that by trying to achieve all of them, the GDPR will fail to achieve any of them. However, when looking closer, one can identify a few core principles the GDPR wants to achieve and does indeed undertake great efforts to achieve them.

15 Jan Philipp Albrecht, in Simitis/Hornung/Spiecker (n 9) Introduction para 185ff; Jan Philipp Albrecht and Florian Jotzo, *Das neue Datenschutzrecht der EU* (1st edn, 2017) 50 para 1; Kühling and Raab (n 9) Introduction para 73.

16 Cf Indra Spiecker gen. Döhmann, 'Information Management' in Peter Cane and others (eds), *The Oxford Handbook on Comparative Administrative Law* (1st edn, 2021) Oxford University Press, 677, 679ff; Rupprecht Podszun and Stephan Kreifels, 'Digital Platforms and Competition Law' [2016] EuCML 33, 38.

17 Case C-131/12 *Google Spain SL og Google Inc v Agencia Española de Protección de Datos (AEPD) og Mario Costeja González* (CJEU, 13 May 2014).

3.1.1 Data Protection as a Safeguard of Democracy

The GDPR identifies as a core regulatory need the regulation of the importance of information for the division of power and thus to avoid power asymmetry based on information. In order for natural persons to be able to execute their freedoms, the political, economic and societal conditions must be construed in a way that allows them to be effective. The amount of information present about an individual, and in close connection to this the individual's knowledge about the information present about her, determines how a business partner, the administration or a third party will assess the individual and make decisions about her. An individual, who is not aware of what is known about her, loses the possibility of self-protection, to give additional information contradicting or strengthening what is already known and to enter into a fair bargain. This individual will not be able to assess her own reactions and the reactions of the other party. In the end, out of insecurity and uncertainty, individuals may refrain from enacting their freedoms if they are unable to assess potential consequences. The newer terminology describes this as "chilling effects": Freedoms and liberties still exist, but their functional enactment is hindered by the circumstances.[18]

Chilling effects not only impact the individual, but the free and democratic society as such. The German Constitutional Court stated this very early on in its ground-breaking census decision.[19] A democratic society can only exist if its members are free to participate and free to enact their freedoms. This constitutes a sphere where the individual is neither under State nor private surveillance. Data protection is then the backbone of a democratic society and guarantees the chance of truly exercising one's fundamental rights.[20]

The GDPR does not explicitly state this relationship between data protection and democracy openly. However, it is well woven into the text and the intention of the Regulation.[21] In recital No. 1, the Regulation sees its foundation foremost in the protection of Art. 8 of the EU Charter and Art. 16 of the Treaty on the Functioning of the European Union (TFEU). The GDPR clearly connects to the DPD, and despite the sometimes polemic description does not fundamentally overhaul the existing data protection regime but rather aims at solving problems not covered by the prior Directive. Recitals Nos. 5, 6 and 7 clarify that the intention of the GDPR is not to loosen the grip of the DPD on data processing but rather to continue, strengthen and fortify its impact.

18 With empirical evidence Jon Penney, 'Chilling Effects: Online Surveillance and Wikipedia Use' (2016) 31 Berkeley Technol L J 117.

19 BVerfGE 65, 1 (43).

20 Indra Spiecker gen. Döhmann, 'Fragmentierungen: Kontexte der Demokratie—Parteien, Medien, Sozialstrukturen' (2018) 77 VVDStRL 9, 55; Benedikt Buchner, in Kühling and Buchner (n 9) art 1 para 13; cf Marie-Theres Tinnefeld, 'Meinungsfreiheit durch Datenschutz—Voraussetzung einer zivilen Rechtskultur' 1 (2015) ZD 22, 22ff.

21 Simitis/Hornung/Spiecker (n 9) Introduction para 235; Spiecker gen. Döhmann (n 20).

What remains open, however, is how far the understanding of data protection as a backbone of freedom and democracy has been intensified and the measures taken to protect it more effectively due to developments on a global scale in comparison to the DPD. After all, global digitality presumes that there have been effects on existing regulatory regimes due to the increased and enlarged use of digital products, infrastructure and services.

What is obvious is the influence of some spectacular events on the EU's regulatory impulse to modernise data protection—most notably the revelations in the course of the NSA scandal in early 2013, but also the decisions of the CJEU in *Google Spain*[22] and *Data Retention*.[23] Nevertheless, these events took place *after* the EU had already decided to reform data protection law in 2009.[24] So, these events have strengthened the impulse that there is a need to protect individuals, and the NSA scandal, *Google Spain* and *Data Retention* have illustrated how quickly the power may shift to few players in the market and to a few States.

The material on the reform process, which started prior to these events, strengthens the understanding that the EU saw changes in the original direction of impact and a need to react. They provide information that the EU did indeed react to some of the changes due to the globality of digitalisation: The European Commission names among other challenges data transfer and a higher enforcement efficiency.[25] The internationalisation of data transfer and data processing, the existence of some global players, in particular in some fields of digitalisation, and the need to protect against these potential aggressors obviously was one of the reasons for action.

3.1.2 Power Asymmetry

The GDPR is also triggered in a more general perspective to react to power asymmetry on the basis of information.[26] Access to information and access to information and communication technology allow for the systematic personalisation and knowledge about individuals and their decisions. Often, knowledge and attributions about persons are construed in a way and with results that

22 Case C-131/12 (n 17); Tobias Herbst, in Kühling and Buchner (n 9) para 67ff; Jan Philipp Albrecht and Florian Jotzo (n 15) 53 para 7.

23 Joined Cases C-293/12 and 594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärtner Landesregierung and Others* (CJEU, 8 April 2014).

24 The Stockholm Programme—an open and secure Europe serving and protecting citizens (2010) OJ C115/01.

25 Commission, 'Communication from the Commission of the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union' COM (2010) 609 final 4.

26 Gerrit Hornung and Indra Spiecker gen. Döhmann, in Spiros Simitis/Hornung/Spiecker (n 9) art 1 para 31.

these persons themselves would never be able to produce as they lack technological and other resources and also the access to them. As a consequence, any entity capable of accessing personal data and of making use of this data receives uncontested power over the individual. The individual, however, is unable to control the data present about her and consequently about any assessments or decisions on this basis. This is in particular true as decisions typically do not reveal which information was used. This entity can be the State, or it can be a private entity.

The DPD and the beginnings of data protection focused in particular on the State and few private actors for reasons of resources. Automated data processing was accessible only to large entities with significant resources and with a large demand of information processing. The GDPR, however, enlarges the perspective. It explicitly takes the availability of information technology in the private sector into focus because of the unprecedented spreading of digital tools and services[27] and thus reacts to the development of digital technology.

While State data processing is exempted to a certain extent because of the dormant opening clause of Art. 6 para. 1 lit. c) and e) GDPR, in Art. 2 para. 2 lit. c) the GDPR fully expands to any private data processing if it is not only for personal or household reasons. Even a quick look through the provisions of the GDPR reveals that much of its regulatory impact has changed focus and is now primarily directed towards private actors, for example, the new chapter on certification applies only to the private sector. Many of the recitals make clear that the GDPR focuses on private data processing. For example, contractual situations are often mentioned in which data processing takes place, or in recital No. 85 the specification of potential risks lists situations which typically occur in the private sector.

Nevertheless, the GDPR continues to address State data processing as well, and the parallel passing of the Directive for the purposes of prevention, investigation, detection, etc.[28] clarifies that the GDPR enacts more than just a simple legal act of the EU but rather is a building block of a digital strategy in which data protection plays an important role—addressing both the Member States and private entities.

Therefore, the attention of data protection law has more clearly integrated data protection against private and state actors; digital globality has taken the EU to a different understanding which has led to a more focused regulatory regime towards private entities without lowering the measures against state actors.

27 Cf Spiros Simitis/Hornung/Spiecker (n 9).

28 Directive 2016/680/EC 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] OJ L 119, 89.

3.1.3 GDPR as Unifier

Recital No. 9 names another reason for the GDPR: It reacts to the consequences of fragmented data protection laws and fragmented enforcement within the EU. While the beginning of the regulation of data processing focused on national approaches and thus individual national law, the DPD addressed a broader audience. It used the interior market clause of Art. 95 of the earlier EC Treaty as an argument to create similar data protection standards in all Member States: The internal market for information (i.e. personal data) should become harmonised. As a number of European States did not have any data protection laws at the time of passing the DPD,[29] this meant the adoption and transfer by those States which already had normative standards for automated decision-making in place and a new regulatory regime for those States which had no standards at all.

Globalisation was, at the time of the passing the DPD, of little importance. The internet did not yet exist in the way we know it today, so data transfer was possible, but with much higher technological hurdles, and also with much less ubiquity in means and addressees as we know today. In 1995, the worldwide acting information companies, mainly with headquarters overseas, were just beginning to develop.

The GDPR, however, recognises changed circumstances. Recital No. 6 explicitly explains that the "scale of the collection and sharing of personal data has increased significantly", and that personal data is now available globally. With this, the GDPR recognises that it has become almost impossible to regulate data processing on a national level and that even regulation on a supranational level encounters difficulties in setting standards and enforcing them. The distribution of data via the internet, internationally available services such as apps, operating systems, hard- and software including the globalised telecommunications infrastructure, and the reliance in many areas of life on mobile services all are intertwined in one interconnected, often (but not necessarily so) interoperable network of information technology. Within this system, data flows frequently and is continuously stored, shared, recombined and altered. A national, even a supranational regulation naturally reaches the limits of control because the different steps of data processing do not necessarily take place within one regulatory regime but are governed by different legal approaches. Consequently, a great uncertainty arises especially among law-abiding controllers regarding which rules are binding for them and which level of data protection they have to guarantee. Often, obligations contradict each other and thus create a choice between Scylla and Charybdis.

In reaction to much of the data processing of European citizens taking place outside the EU, the GDPR enlarges its territorial scope in comparison to the

29 Spiros Simitis/Hornung/Spiecker (n 9) Introduction para 88; Martin Selmayr and Eugen Ehmann (n 10) Introduction para 57; Jochen Schneider, in Jochen Schneider (ed), *Handbuch EDV—Recht* (5th edn, 2017) Dr. Otto Schmidt, A para 46.

DPD. This aspect of the GDPR as a unifier will be discussed later in the chapter on territorial scope (3.3.2). However, the effect goes beyond enlargement of territoriality: Art. 3 para. 2 GDPR also makes clear that the EU considers its legal standard as binding worldwide for every controller. One can also conclude from the standards for data transfer outside the EU that the GDPR is considered to be the gold standard: Although it is sufficient to have an adequate standard of protection under Art. 44 et seq. GDPR for enabling personal data to be processed outside the EU, the CJEU has upheld and fortified its decisions on when adequacy can be assumed in prominently striking down both the so-called Safe Harbor Agreement[30] and the so-called Privacy Shield.[31] Both agreements were the basis of transatlantic data transfer which came to a halt due to these decisions.

As a result of the strengthened self-esteem of EU data protection law, international actors have reacted. From an outsider's viewpoint, the GDPR has a unique selling point in being the most comprehensive and citizen-protecting data protection law so far, offering one of the few tools to create a level playing field in information law. Therefore, it is not surprising that the international interest in the GDPR is big, and that quite a few influential States have taken political action on the basis of the GDPR. Naming the big three—California, Japan and Brazil—which have all passed GDPR-inspired and often look-alike regulations, illustrates this convincingly. Even States with little democratic interest but with highly rated economic interests in doing business with the EU have adjusted, even if only pro forma or only in regard to the private and not the public sector.

In the end, the GDPR so far—and the process is dynamic and not yet finished—has started a global process of raising the awareness of data protection once more. It may even serve as a unifier: Within the EU, this is certainly true, globally, one will have to see.

3.2 Core Regulatory Instrumental Approach

The approach of the GDPR in comparison to that of the first regulatory regimes in data protection law has changed. It has already been pointed out that the regulation of private entities (businesses, etc.) has become an important factor, while State regulation is still prominent but due to the particularities of EU competence law not as prominent. The protection of personality and autonomy as the backbone of democracy is in part now addressed in other regulations, such as

30 Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) [2000] OJ L 215/7.

31 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176) [2016] OJ L 207/1.

media law or hate speech regulation. Nevertheless, data protection still remains an important tool to protect these core freedoms.

This chapter will illustrate changes in two core regulatory instruments: It shows that the precautionary principle is in some regards reformulated as a risk-based approach. The GDPR also introduces more openly a consumer protection approach and uses data protection law as a new tool and vehicle for control of fair markets and fair trade.

3.2.1 Precautionary Principle Versus Risk-Based Approach and the Concept of Technological Neutrality

The early data protection legal regimes followed a technology law-based approach (i.e. foremost the precautionary principle but also other instruments such as state control by authorities). They embraced the idea that any type of data protection could cause risks. The statement of the German Constitutional Court in its ground-breaking 1983 census decision is typical of this: "There is no irrelevant data".[32] Consequently, the DPD stated that any type of data processing needed a justification; otherwise, it was considered to be illegal and lack legitimate grounds. This approach has often been described as making use of the standard approach of law-and-order from administrative law, the concept of the principle of prohibition with the reservation of permission:[33] A private activity is forbidden, but the State can allow it on legitimate grounds for particular superior legal interests, among them individual freedoms and liberties.

It should be noted, however, that this interpretation had some flaws from the beginning: First, private entities, which were also addressed by the DPD, act under the principle of freedom. Different from the State, they need no justification for any action but just the opposite: The State has to justify infringement of fundamental rights of private entities which a law-and-order regulatory regime clearly constitutes. Such a principle of prohibition would thus only be easy to establish if it addressed merely the State, as it is bound by the rule of law.[34] Thus, the State needs a legal ground for restrictions of the liberties of citizens (i.e. any infringement of data processing). But for private entities and persons, such a general principle of prohibition requesting a permission from the State authorities would be considered to be an intense interference with their basic freedoms. A pragmatic argument against such an interpretation is also that the DPD never included an active and full procedure for permission. This would have reduced

32 BVerfGE 65, 1 (16, 43).

33 Heinrich Wolff, in Stefan Brink and Heinrich Wolff (eds), *BeckOK Datenschutzrecht* (35th edn, 2020) C.H.Beck, Basics para 18; Heinrich Amadeus Wolff, in Peter Schantz and Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, 2017) C.H.Beck, D para 389; Jan Philipp Albrecht and Florian Jotzo (n 15) 50 para 2; Jürgen Kühling and Johannes Raab, (n 9) Einführung para 52ff.

34 In Germany, Grundgesetz (GG) art 20 sec 3.

data processing activities to a minimum, and neither of the early (and also the present) data protection legal regimes intended this.[35]

True is, however, that the requirement of justification newly enshrined in the DPD turned the general approach to data processing around. Now, private entities and States had to control their activities and *ex ante* perform at least a rough test as to whether their data processing was legal under the DPD and the transposition into law by Member States. As the application of the DPD was broad ("any personal data"), this meant a considerable effort on the part of data processors. This need for preventive measures was enlarged even further by the fact that the DPD did not distinguish between certain types of data processing or grant privileges to particular data processing. Rather, "technological neutrality" was the declared regulatory strategy: The DPD was designed to be applicable to any data processing in general, as the latent possibility of recombination of data poses a continuous threat to any data.[36]

The GDPR in general upholds this approach but it does not embrace it as strictly as did the DPD.[37] Rather, it has included a number of provisions in which it assumes that there are specific types of data processing which can be considered to be riskier than others in regard to the concepts of data protection. Here, a more risk-based approach can be identified, even if it has not been taken over within the GDPR completely.[38] In consequence, there will be a development in the coming years where riskier operations will be controlled and regulated further while other types of data processing will not gain as much attention from controllers and supervisory authorities.

One of these provisions illustrating the additional risk-based approach can be found in Art. 35 GDPR, the so-called "data protection impact assessment".[39] Article 35 introduces an instrument for early warning,[40] by which the controller is required to assess the riskiness of a data processing and consequently proactively install measures to reduce the risks. The controller may also have

35 Cf Alexander Roßnagel, in Spiros Simitis/Hornung/Spiecker (n 9) art 5 para 35ff; different view: Peter Schantz, in Schantz/Wolff (n 33) art 5 para 5; Philipp Kramer, in Martin Eßer and others (eds), *Auernhammer: Datenschutz-Grundverordnung: Bundesdatenschutzgesetzt und Nebengesetze: Kommentar* (7th edn, 2020) Carl Heymanns, art 5 para 10.

36 Gerrit Hornung and Indra Spiecker gen. Döhmann, in Spiros Simitis/Hornung/Spiecker (n 9), Introduction para 242; Jochen Schneider, in Jochen Schneider (ed), *Handbuch EDV—Recht* (5th edn, 2017) Dr. Otto Schmidt, A para 31.

37 Gerrit Hornung and Indra Spiecker gen. Döhmann, in Spiros Simitis and others (n 9) Introduction para 242.

38 Ibid para 242.

39 Moritz Karg, in Spiros Simitis and others (n 9) art 35 para 1; Axel Freiherr von dem Bussche, in Kai-Uwe Plath (ed), *DSGVO BDSG Kommentar* (3rd edn, 2018) Dr. Otto Schmidt, art 35 para 1; Silke Jandt, in Jürgen Kühling and Benedikt Buchner (n 9) art 35 para 1.

40 Moritz Karg, in Spiros Simitis and others (n 9) art 35 para 2; Bertram Raum, in Martin Eßer and others (n 35) art 35 para 2; Mario Martini, in Boris P Paal and Daniel A Pauly (eds), *Datenschutz-Grundverordnung* (3rd edn, 2021) C.H.Beck, art 80 para 1.

to consult the supervisory authorities. Article 35 para. 3 GDPR enumerates a number of data processing types which are per se considered to be of high risk, among them profiling (lit. a)) or data processing in regard to special categories of data (lit. b)). Article 35 para. 4 GDPR also requires that supervisory authorities publish lists of those data processing types which fall under the obligation of undergoing an Art. 35 GDPR risk assessment. The authorities are also enabled by Art. 35 para. 5 GDPR to publish an equivalent list of processing types not considered to be risky in the sense of Art. 35 para. 1 GDPR. These lists do not only specify the obligations of controllers in regard to these listed activities, but also serve as examples for interpretation of other, not listed processing types.

The legal definition of particular risky data processing types, as well as the possibility to define activities as not risky, derogates from the original principle that it is the concise circumstances which produce risks for the liberties and freedoms of individuals, and thus any data processing has to be judged individually. Under Art. 35 GDPR, however, the exact controller, the concise purposes and the specific data processing technology now only matter once the threshold of a risk assessment has been undertaken.

3.2.2 Data Protection Law as Consumer Protection and Fair Competition Law

A change of the core regulatory approach can also be identified in regard to the regulatory regime and the regulatory goals of EU data protection law. The DPD was originally a technology-regulation tool aiming at controlling an emerging technology. It employed the characteristic instruments, the precautionary principle being the most prominent one, establishing an *ex ante* regulatory regime and supervisory authorities among others. Controllers were required to test their data processing activities prior to undertaking them: On a primary level, controllers fell under obligations to restrict their activities. Today, the principle of legality in Art. 5 para. 1 and Art. 6 para. 1 GDPR are at the centre of this understanding.

The DPD did not distinguish between the different groups of actors other than between data controllers (including data processors) and data subjects. Data subjects per se were considered to be caught in informational power asymmetries in comparison to data controllers. The particular circumstances in which these power asymmetries arose were not part of the regulatory design.

This is now different with the GDPR—at least some provisions identify different subgroups of protection-worthy situations. Elements of consumer protection law and competition law have been introduced, most prominently in the provision of Art. 20 GDPR regarding the right to data portability.[41] A majority of current EU directives define the consumer as a "natural person who is acting for

41 Cf Alexander Dix, in Spiros Simitis and others (n 9) art 20 para 1; Hans-Georg Kamann and Martin Braun, in Martin Selmayr and Eugen Ehmann (n 10) art 20 para 3; Tobias Herbst, in Jürgen Kühling and Benedikt Buchner (n 9) art 20 para 4.

the purposes which are outside his trade, business and profession".[42] Consumer protection law addresses a fundamental problem, mostly in contractual circumstances: Consumers find themselves often in situations where they do not bargain from an equal position, especially with large corporations and industries in business transactions. These transactions typically concern their private lives, but they are inherently disadvantaged. Thus, consumer protection law aims at protecting consumers from serious risks and threats that they are unable to tackle as individuals; at empowering them to make choices based on accurate, clear and consistent information; and finally at enhancing their welfare and effectively protecting their safety as well as their economic interests.[43] The EU has a longstanding tradition of protecting consumer interests.

Although the GDPR does not explicitly name the "consumer" as a subgroup of data subjects, the core goals of data protection to counteract informational power asymmetry and of consumer protection law to counteract power asymmetry on the marketplace are naturally closely linked. This holds true even if data protection law does not take economic effects as a starting point as does consumer protection law. Data protection law is thus larger in application as it takes into account effects of informational power asymmetry on any type of decision. Nevertheless, some of the instruments of data protection law can be observed similarly in consumer protection law, especially strengthening organisational control of conditions, assisting consumers/data subjects to make better choices and effectively pursue their rights against unfair practices. It is thus not surprising that supervisory authorities have already identified a connection between data protection and consumer protection prior to enactment of the GDPR.[44]

The new Art. 20 GDPR is the final open link of data protection to consumer protection. It addresses the very special problem of the so-called "lock-in effect", in particular observed with networks and platforms, most prominently with the social networks.[45] The provision establishes a new right for data subjects to request from controllers the receipt of personal data and the transfer of this data to another controller. This right has been criticised as being too narrow

42 Jane Valant, 'Consumer Protection in the EU. Policy Overview' (European Parliament (EPRS), 4 September 2015 <www.europarl.europa.eu/RegData/etudes/IDAN/2015/565904/EPRS_IDA(2015)565904_EN.pdf> accessed 22 May 2021.

43 Ibid 3.

44 Cf for Germany the resolution of the German National Data Protection Conference: 'Entschließung Marktmacht und informationelle Selbstbestimmung, 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 08./09. Oktober 2014' 23ff <www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/88DSK_Marktmacht.html?nn=5217228> accessed 23 May 2021; for the EU art 29-Working Group Guidelines on the Right to Data Portability (2017) WP 242 rev 01, 4.

45 Alexander Dix, in Spiros Simitis and others (n 9) art 20 para 1; Gerrit Hornung, 'Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012' (2012) 3 ZD 99, 103; Tobias Herbst, in Jürgen Kühling and Benedikt Buchner (n 9) art 20 para 2.

to really counteract the "lock-in effect" as Art. 20 GDPR does not require interoperability.[46]

Nevertheless, Art. 20 GDPR opens the door to data protection law as a tool to correct dysfunctionalities on the market of information goods and services. The provision thus openly includes instruments of market design which change the rules of business.

The "lock-in effect" creates an obstacle to effective competition; it creates high burdens on market entry. Being a countermeasure, Art. 20 GDPR actively links data protection law to competition law. The discussion of the relation between the two legal regulatory regimes has—at least in Germany and Europe—so far been addressed more from the side of competition law. Most prominently, the issue has been raised by the Federal Cartel Office (Bundeskartellamt), Germany's highest competition authority: In a decision against Facebook, it used data protection law effects as the core argument for a rule against the company's practice of recombining user data from different sources inside and outside the corporate group.[47] Data protection law with its goal of the highest effectiveness of protection of the data subject's rights does not bar additional safeguards from other legal regimes. Recital 146 of the GDPR thus declares that data protection liability exists "without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law".

The enlargement of the regulatory regime towards additional consumer safeguarding can be identified as a reaction to global digitality: Internationally operating IT companies have enlarged the power asymmetry not only towards data subjects in general, but in consumer relations in particular.

3.3 Content Regulation

Having so far elaborated on the general principles, the regulatory approach and core goals of the GDPR, it is fair to state that new EU data protection law has extended the concepts of data protection under conditions of globality. A further look at particular actions within the individual provisions of the GDPR will show further reactions in detail.

3.3.1 Enforcement Deficit

Among the impulses on the part of the EU to reform the existing data protection regulatory regime was the desire for a better harmonised, if not even unified, legal

46 Alexander Dix, in Spiros Simitis and others (n 9) art 20 para 1; Tobias Herbst, in Jürgen Kühling and Benedikt Buchner (n 9) art 20 para 3.

47 'Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources' (2019) <www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html;jsessionid=7630FEA430282799A5AF10176B4F668B.1_cid362?nn=3591568> accessed 22 May 2021; BGH GRUR 2020, 1318.

status enforcement of the existing legal status in comparison to the DPD.[48] In the course of time, it had become obvious that, in particular, the enforcement mechanisms provided by the DPD and the transposition into law by Member States were not sufficient to provide for execution of the provisions to effectively protect personal data.[49]

The reasons for this were many. It was unclear which tasks, competences and powers the supervisory authorities had. Some involved parties and States were of the opinion that the DPD did not grant to supervisory authorities the power to enact individual rules and to enforce them; other Member States had established extensive competences and powers. This, but also different traditions, understandings and interpretations, led to diverging assessments and decisions of supervisory authorities in the Member States on similar or even the same data processing types. This created uncertainty and reduced the effectiveness of enforcement. This effect was intensified on an international level due to the effect of "data protection law shopping", especially by large and internationally operating companies in search of a minimally enforcing Member State interpretation of the DPD. In particular, large international information corporations had pushed enforcement through and cooperation between supervisory authorities to the limit. They had designed corporate and technical structures to avoid application of the DPD or only limited data processing being under the regime of the Member State and DPD jurisdiction.

Especially this latter fact is directly linked to the effects of the global digitality: As most of the digitalised services are offered internationally and the most important companies are headquartered outside the EU, any enforcement deficit is also a straightforward result of the globalised, mostly internet-based digitalisation system. It is also directly linked to the applicability of the DPD and Member State data protection law. This will be dealt with next.

In addition to this, violations of the DPD and Member State law were often hardly sanctioned. For example, in Germany, liability for breach of data protection laws was factually non-existent, as German law in general allows recovery only for material damages and thus typically does not grant data subjects effective damages for personality or informational rights' violations. The possibility of levying fines was often restricted in the Member States. Thus, secondary law often had no governing effect to effectively sanction violators.

In reaction to these legal problems, the GDPR takes great efforts in reform in order to provide effective enforcement. The efficiency of supervisory authorities has been strengthened and their competences and powers have been clearly stated in the enumeration of Art. 55 et seq. GDPR. In order to unify the assessment of data processing types, the European Data Protection Board (EDPB) formalised the idea of the Art. 29 Working Group under the DPD. The consistency

48 COM (2010) 609 final (n 25) 4.

49 Cf Moritz Karg, in Stefan Brink and Heinrich Wolff (n 33), art 80 para 6; Eike Michael Frenzel, in Boris P Paal and Daniel A Pauly (n 40).

mechanism, Art. 63 et seq., together with the creation of a leading supervisory authority, establishes a procedure by which binding decisions among the different authorities are made possible and in some instances are even mandatory.

In order to effectively detect data protection violations, the rights of data subjects have been enlarged in comparison to the DPD, and in Art. 12 et seq. GDPR information rights have been described more precisely. Damages, including immaterial damages, are now explicitly addressed in Art. 82 para. 1 GDPR. Also, Art. 80 GDPR newly provides for representation of data subjects in enforcement procedures similar to a representative action.

It should also be noted that enforcement-related obligations are strengthened additionally by the duty to demonstrate legality as stated in the new Art. 24 para. 1 GDPR: This requires every controller to document properly that any processing is performed in accordance with the GDPR. Thus, even potential procedural problems are addressed.

3.3.2 Territorial Scope

One important aspect of the problem of a lack of strict and foreseeable enforcement was the restriction of the mostly territorial scope of data protection law within the EU. The DPD followed a principle of territoriality, that is, any—but also only—data processing taking place within the EU was regulated under EU law. This principle was accompanied by the principle of establishment, that is, any data processing performed in the context of the activities of an establishment in the EU had to act in accordance with the DPD and the transposition into law by Member States.

This, however, proved to be problematic in all cases where data subjects offered their data to controllers outside the EU who did not have an establishment within the EU. Many international controllers had thus created establishments within the EU by which their marketing and business activities were performed, but the core data processing was taking place outside the EU. By this approach, many international companies were able to avoid the regulatory impact of EU data protection law.

The GDPR reacts to this development by forsaking the principle of territoriality in favour of the so-called "marketplace rule", Art. 3 para. 2 GDPR. The marketplace rule makes EU law applicable to anyone offering goods or services to individuals in the EU—regardless of a financial or contractual obligation involved—or monitoring the behaviour of persons within the EU. Thus, neither territoriality nor establishment are mandatory, and thus a material relationship with the EU in processing is no longer necessary.

This change is of particular importance for the effects of global digitality, and this is so for two reasons. The first reason is the obvious one: The GDPR, as opposed to the DPD, now applies to any data processing that addresses natural persons within the EU and thus deviates from the prior principle of territoriality. Now it is no longer necessary to actually prove a data processing within the EU in order to call for protection from the GDPR.

The second aspect revealed by this new Art. 3 para. 2 GDPR is a remarkable development in the handling of digital goods and services. By applying the marketplace principle, the legislator paralleled the application of EU law in regard to virtual goods and services and their effects with non-virtual goods and services. Both now follow the legal regime that anything—material products as well as virtual services—entering the EU are required to adhere to EU standards: A US car must fulfil all requirements of EU product and safety regulations; this is now likewise the case with any online service offered to someone in the EU.

Thus, we can observe a shift on the part of the EU to master not only its own marketplace but to react to international companies having conquered successfully the turf of digital services and goods—an aspect that the EU was not strongly committed to under the DPD.

3.3.3 Enforcement of the Enforcement

The GDPR actively seeks to master the enforcement deficit which had arisen under the DPD. As illustrated, a number of tools have been selected in order to not only formulate material standards but also to assure that these standards are binding and enforced.

However, one aspect the GDPR does not address and thus continues to follow the lead of the DPD is in the "enforcement of the enforcement" (i.e. how to ensure that any type of measure any controller has been obliged to take is actually taken). Also, there is a lack of instruments on how to enforce sanctions of any kind, foremost fines and damages.

Here, the GDPR continues to rely on general legal provisions (i.e. rights of access and information, etc.), in general international and Member State procedural and enforcement law, and the established venues for enforcement (i.e. courts and then enforcement agencies). This means, however, that any of the instruments of the GDPR, which need further enforcement or control, will run into the same difficulties as known in other areas of law, as well. It is international law which governs to what extent internationally operating entities can truly be forced to adhere to rules within the EU.

3.3.4 Internet Regulation

It will only be touched on briefly that the GDPR also does not address the internet and its specific problems with respect to data protection explicitly. Many new regulatory tools are obviously a reaction to the development of the internet and its ubiquity. However, the technology-neutral approach of the Regulation is probably best seen in the refusal to state a specific content regulation.

Just how difficult it is to reach a mutual understanding in this regard is illustrated by the not-concluded debate about a new ePrivacy Regulation, which was meant to provide exactly such internet-specific regulation on the basis of the GDPR. Despite many efforts by several presidencies within the EU, no compromise has been reached thus far. So, the GDPR remains the essence of data

protection without addressing the specificity of internet regulation. Here, global digitality has arrived in theory, but not in practice.

4 Conclusion and Outlook

The conclusion of this first and short analysis, restricted to some general ideas and instruments in EU data protection law, is the following: Data protection law has not turned into a "new" law in the course of increased and of global digitality. Rather, one can observe the field as a dynamic area of law which has adjusted in some parts to developments over the past 30 years and in particular to the increased international operations in information technology. However, sovereignty and international law take its toll: The EU has expanded its substantive law approach and the immediate enforcement of it by several instruments, but not the actual "enforcement of the enforcement". Overall, data protection law remains the most comprehensive information law there is—and the GDPR, following in the footsteps of the DPD, is a powerful tool to regulate digitality also on a global scale. This is true not the least because of its model character, which many States worldwide have started to align with when intensifying their own data protection efforts.