Current Legal Problems, Vol. XX (2023), pp. 1–47
https://doi.org/10.1093/clp/cuad009
Advance Access published 10 October 2023

Complete and Effective Data Protection

*Orla Lynskey**

Abstract Data protection law is often invoked as the first line of defence against data-related interferences with fundamental rights. As societal activity has increasingly taken on a digital component, the scope of application of the law has expanded. Data protection has been labelled 'the law of everything'. While this expansion of material scope to absorb the impact of socio-technical changes on human rights appears justified, less critical attention has been paid to the questions of to whom the law should apply and in what circumstances. The Court of Justice has justified an expansive interpretation of the personal scope of the law in order to ensure 'effective and complete' data protection for individuals. This article argues that the attempt to make the protection offered by the law more 'complete' risks jeopardising its practical effectiveness and raises doubts about the soundness of the regulatory approach to data protection. In the quest for effective and complete protection, it seems that something must give.

Key words: data protection; privacy; regulation; enforcement; compliance; effectiveness

1. *Introduction*

The right to data protection enjoys a privileged position in the EU legal order.[1] The right is strictly interpreted by the Court of Justice of the EU (CJEU) and is given remarkable weight when balanced with other rights and interests.[2] While data protection sits alongside the more established

* Associate Professor, LSE Law School and Visiting Professor, College of Europe Bruges, Belgium. E-mail: O.Lynskey@lse.ac.uk. I am very grateful to the Editors of Current Legal Problems for the invitation to contribute to this series, with particular thanks to Despoina Mantzari for her guidance throughout. My thanks also to the anonymous referees for their valuable comments and to Mr Wojciech Wiewiórowski, the European Data Protection Supervisor, for his generosity in attending and chairing the lecture. I benefited from helpful feedback on earlier drafts of this text from Gloria Gonzalez Fuster, Hielke Hijmans, Filippo Lancieri, Rotem Medzini, Katherine Nolan and Thomas Streinz. All views, and any errors, remain my own.

[1] Bilyana Petkova, 'Privacy as Europe's First Amendment' (2019) 25 *European Law Journal* 140.

[2] For instance, in *Google Spain* the Court held that 'as a general rule' the data subject's rights to data protection and to respect for private life override the interests of internet users in access to information (Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317, para 81).

right to respect for private life in the EU Charter,[3] it is data protection rather than its more established counterpart that is specifically referenced in the EU's General Data Protection Regulation (GDPR). The GDPR, like its predecessor a 1995 Directive, has influenced the adoption of European-style data protection laws globally.[4] Recently adopted EU legislative initiatives in the digital sphere, such as the Digital Markets Act[5] and the Digital Services Act,[6] are all 'without prejudice to' the GDPR.[7] Data protection is, therefore, both a cornerstone of EU digital regulation as well as its international poster child and is treated as an 'issue of general and structural importance for modern society'.[8] Yet, set against this success story of EU data protection law, recurring reservations have been expressed about both its boundaries and its capacity to achieve its objectives in practice.[9]

A key concern is that EU data protection has become the law of everything applied to everyone putting compliance with the legal framework, and those charged with its enforcement, under strain. This development of the law is driven, to a large extent, by the jurisprudence of the CJEU. Scholars attribute the broad scope of the law to the need to

[3] Gloria Gonzalez Fuster and Hielke Hijmans, 'The EU Rights to Privacy and Personal Data Protection: 20 Years in 10 Questions', VUB Discussion Paper (2019) https://cris.vub.be/ws/portalfiles/portal/45839230/20190513.Working_Paper_Gonza_lez_Fuster_Hijmans_3_.pdf.

[4] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020) 132; Anu Bradford, 'The Brussels Effect' (2012) 107 Nw U L Rev 1, 22–26. The Council of Europe's Convention 108 is also a highly influential instrument and a likely standard for global convergence; Global Privacy Assembly, 'Privacy and Data Protection as Fundamental Rights – A Narrative' https://globalprivacyassembly.org/wp-content/uploads/2022/03/PSWG3-Privacy-and-data-protection-as-fundamental-rights-A-narrative-ENGLISH.pdf, 48–50.

[5] 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) (Text with EEA relevance) OJ [2022] L265/1.

[6] 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) (Text with EEA relevance) OJ [2022] L277/1.

[7] Ibid, Article 2(4)(g) and recital 10. This also follows from recital 12 and Article 8(1) Digital Markets Act (n 5).

[8] Peter Hustinx, 'The Role of Data Protection Authorities' in Serge Gutwirth et al. (eds), *Reinventing Data Protection* (Springer 2009) 131, 133.

[9] From within the Court see, for instance, Case C-245/20, *X, Z v Autoriteit Persoonsgegevens* ECLI:EU:C:2021:822, Opinion of AG Bobek, paras 55–56. Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) *Law, Innovation and Technology* 40; Bert-Jaap Koops, 'The Trouble with European Data Protection Law' (2014) 4 *International Data Privacy Law* 250.

protect fundamental rights in the context of significant socio-technical changes.[10] Since the 1970s, when data protection laws were first adopted, these laws have sought to address the risks and harms for fundamental rights that stem from personal data processing.[11] At that time, the primary focus was on mitigating the adverse effects that might follow for individuals from holding and controlling files on them and combining information across databases and computer systems.[12] Although, these concerns are still present, the technological and societal landscape has shifted dramatically. Advances in automation, such as the widespread availability of generative AI, will further unsettle the environment to which the law applies and which shapes its application.

To date, the law has expanded to absorb the impact these socio-technical changes might have on fundamental rights with the Court emphasising the need for 'effective and complete' data protection in its jurisprudence. This article argues that the broad personal scope of application of the law—the attempt to make the protection offered by the law more 'complete', in the language of the Court—risks jeopardising its practical effectiveness and raises doubts about the soundness of the regulatory approach to data protection.[13] In the quest for effective and complete protection, it seems that something must give. While a broad application of the concept of personal data is necessary to protect fundamental rights in light of socio-technical developments, the legislature may need to revisit to whom the law applies and what obligations adhere to distinct controllers under the legal framework. This inquiry also illuminates the need for further reflection and research on the relationship between the law's scope, compliance with the law by its addressees and its enforcement by regulators.

This argument proceeds in three parts. First, it outlines why it is now argued that data protection has become the law of everything but

[10] Colin J. Bennett and Robin M. Bayley, 'Privacy Protection in the Era of "Big Data": Regulatory Challenges and Social Assessments' in Bart van der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016) 205, 210.

[11] Raphaël Gellert, *The Risk-Based Approach to Data Protection* (OUP 2020), 186.

[12] Luca Tosoni, 'Article 4(6): Filing System' in Christopher Kuner, Lee A Bygrave, Christopher Docksey and Laura Drechsler (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 138, 141.

[13] The expansive approach to the territorial application of the GDPR is justified on the same grounds but is beyond consideration of the jurisdictional reach of the rules is beyond the scope of this article. On jurisdictional issues see, Merlin Gömann: 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) *Common Market Law Review* 567.

suggests that the more significant development is the application of the law to everyone, with few exceptions to its material and personal scope of application. While existing legal literature has queried whether the law should apply to everything, much less attention has been dedicated to the question of whether everyone should be subject to the same legal obligations. Second, it demonstrates that this ideal of complete protection is leading to cracks in the legal framework and suggests that these cracks are currently being patched over by Courts and regulators in a way that is itself antithetical to effective data protection. Third, it interrogates whether some of these problems might be addressed by adopting a more flexible approach to data protection interpretation and enforcement. This approach itself raises fundamental questions that must be addressed, suggesting the time may be ripe for a more radical rethink of the data protection framework.[14]

2. *The Law of Everything Applied to Everyone*

Data protection is a regulatory regime that puts in place a series of both rules and principles that must be applied whenever personal data is processed. It regulates the creation, collection, storage, use and onward transmission of personal data, amongst others.[15] At its most basic, when the data protection framework applies, personal data processing can be legitimised if certain conditions are met: there must be a legal basis for processing and adherence to the principles of fair data processing.[16] The legal framework thus imposes compliance obligations primarily on 'data controllers' and grants rights to individuals ('data subjects').[17] An innovation in the GDPR is the introduction of a suite of meta-regulatory obligations, including an obligation of demonstrable accountability applicable to controllers and various other compliance requirements such as the need to conduct data protection impact assessments and to

[14] Before the enactment of the GDPR Erdos remarked that its 'almost unfathomable scope, inflexible nature and sometimes unduly onerous default standards' are ill suited to digital realities, recommending a more radical shift of focus and balance in the law. David Erdos, *European Data Protection Regulation, Journalism, and Traditional Publishers: Balancing on a Tightrope?* (OUP 2019) 146.

[15] Colin Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press 1992).

[16] Articles 5 and 6 GDPR.

[17] Articles 12–22 GDPR.

appoint a data protection officer (DPO) in some circumstances.[18] In the EU, this legislative framework is undergirded by the right to data protection found in the EU Charter of Fundamental Rights.[19] The Court has held in its caselaw that the very act of personal data processing engages the right to data protection and must therefore comply with the requirements set out in Article 8 EU Charter.[20] The legislative framework could therefore be viewed as something that simultaneously facilitates the interference with a fundamental right while allowing for the justification of this interference if its legal requirements are satisfied.[21] From a human rights law perspective, the entire legislative framework functions as a justificatory regime. The implicit aim of the legal framework is to ensure that data processing operations are proportionate in that they pursue a legitimate aim and contain safeguards to ensure they do not go beyond what is necessary to achieve that aim.

Since the adoption of data protection laws by the EU in 1995, the data protection framework has been characterised by its expansive scope of application. The key concepts determining the material scope of application of the EU system are defined broadly, with exceptions construed narrowly. It follows that as societal activity now increasingly has a digital component, data protection has become an almost unavoidable legal framework[22]: data protection is the law of everything,[23] applied to everyone. This is, however, as much a result of a legal evolution as it is a socio-technical one. This section will trace how this has come to pass. The material and personal scope of the rules are defined and interpreted

[18] Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach' (2018) 9 *European Journal of Risk Regulation* 502; Reuben Binns, 'Data Protection Impact Assessments: A Meta-regulatory Approach' (2017) 7 *International Data Privacy Law* 22.

[19] On the phenomenon of legislative instruments giving expression to fundamental rights in equality and data protection law see Elise Muir, *EU Equality Law: The First Fundamental Rights Principle of the EU* (OUP 2018) 137–143.

[20] Joined Cases C-293/12 and 594/12, *Digital Rights Ireland Ltd and Seitlinger and others* EU:C:2014:238, para 36. See also C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* EU:C:2020:559, para 170; Opinion 1/15, ECLI:EU:C:2016:656, para 123.

[21] The Court has conceptualised the application of the right to data protection in this way, however, the content and application of the right remain contested. See, González Fuster and Hijmans (n 3).

[22] While it remains possible to envisage daily activities that do not entail personal data processing, such as riding a bicycle or reading a book, a digital component is now introduced to many of our activities (such as the digital transactions required to rent a bike in a city or the use of an e-reader to read books).

[23] This term was coined by Purtova in her influential article 'The Law of Everything' (n 9).

expansively while exceptions to their scope have been construed restrictively. Moreover, attempts to limit this expansionist approach have been rejected by the CJEU. Later sections will explore the implications of this expansionist approach for effective data protection.

A. *The Law of Everything*

Data protection law applies to the processing of personal data. Any operation or set of operations performed upon personal data, whether by automatic means or not, constitutes processing. It is therefore difficult to conceive of any type of activity with a digital component that would not constitute processing.[24] The only limitation found in the law is that where the processing is conducted manually, as opposed to fully or partly automated processing, the data processing must form part of a filing system which allows for the easy retrieval of an individual's data file.[25] For the law to apply, however, it is *personal* data that must be processed.

Data protection law operates in a binary way: it applies when the data processed are classified as 'personal' data but does not apply to the processing of non-personal data.[26] Much therefore hinges on what is classified as 'personal data'. Anonymous data is not treated as personal data whereas data that is pseudonymised, where the data can only be attributed to a specific individual once combined with additional information which is separately held and subject to additional measures to ensure non-attribution, is personal data.[27] The scope of the term personal data is wide, as we shall see, and what constitutes personal data is varied.[28] Personal data is defined as 'any information relating to an identified or identifiable natural person'.[29] While much of the focus in the

[24] Damian George, Kento Reutimann and Aurelia Tamò-Larrieux, 'GDPR Bypass by Design? Transient Processing of Data Under the GDPR' (2019) 9 *International Data Privacy Law* 285.

[25] Article 4(6) GDPR defines a 'filing system' as 'any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis'.

[26] The GDPR recognises a category of pseudonymous data but this is still categorised as personal data (Article 4(5) GDPR).

[27] Recital 26 GDPR. Article 4(3)(b) GDPR defines pseudonymisation.

[28] See, for instance, the examples recognised in the Court's jurisprudence referred to by Wachter and Mittelstadt in Sandra Wachter and Brett Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI' (2019) *Columbia Business Law Review* 1, 30–31.

[29] Article 4(1) GDPR.

existing doctrine is on the issue of identifiability[30]—what does it mean for an individual to be identified and when is an individual identifiable—the other elements of the definition may be equally consequential for its application. Indeed, while it is necessary to disaggregate these elements in order to apply this definition, it is only by considering them together that the overall reach and impact of the law can be determined. Some examples may help to illustrate these points.

Many publishers describe the peer review process as anonymous on the basis that the data being processed—in this case the article distributed for peer review and the comments of the reviewers—do not reveal the identity of the individuals at stake.[31] Anonymity in this colloquial sense is distinct from anonymity as defined in the GDPR. In the peer review context, individuals are deemed anonymous if they cannot be identified or identifiable from the data immediately available to authors or reviewers (an errant reference to previous work revealing an author's identity, for instance).[32] However, for GDPR purposes, irrespective of whether the article or review allowed for an individual's immediate identification, they would meet the legal standard for identifiability. An individual is considered identifiable where they can be identified, directly or indirectly using means reasonably likely to be used by the data controller or by any third party. In this example, the identifiability threshold is easily met as the journal editor is able to identify both the author of the article and the reviewer even where they remain unknown to one another. We might be tempted to stop the analysis here, however, the remaining elements of the definition must also be met. If an unreliable author submitted a piece of work that had been generated by ChatGPT and contained inaccuracies attributed to non-existent

[30] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2009) 57 *UCLA Law Review* 1701; Michèle Finck and Frank Pallas, 'They Who Must Not Be Identified—Distinguishing Personal from Non-personal Data Under the GDPR' (2020) 10 *International Data Privacy Law* 11; Nadezdha Purtova, 'From Knowing by Name to Targeting: The Meaning of Identification Under the GDPR' (2022) 12 *International Data Privacy Law* 163.

[31] See, Taylor and Francis, 'What Are the Different Types of Peer Review?' https://authorservices.taylorandfrancis.com/publishing-your-research/peer-review/types-peer-review/; or OUP, 'Five Models of Peer Review: A Guide' (23 September 2021) https://blog.oup.com/2021/09/five-models-of-peer-review-a-guide/.

[32] Anonymity in this context serves the purpose of limiting the risk of bias in the evaluation procedure (as distinct from under the GDPR where it serves to determine the law's scope of application).

sources this would nevertheless constitute 'information'.[33] Instinctively, we might also think that an academic article could not be personal data as its content is not about a particular academic, it is simply the output of their efforts. Early caselaw in the UK, for instance, insisted that personal data must focus on an individual or be biographical in a significant sense.[34] However, the Court endorsed a much more capacious vision of personal data in *Nowak* finding that information can relate to an individual in so far as it is linked to the individual by reason of its 'content, purpose or effect'.[35] In *Nowak*, the CJEU considered that the examination script of a candidate in an open book examination 'related to' the candidate as the content of the answers reflected the extent of the candidate's knowledge and competence; the purpose of the processing was to evaluate their professional abilities and suitability for practice and the use of that information would be liable to have an effect on their rights and interests.[36] The Court also held that the examiner's comments related to the candidate as, amongst others, their purpose is to record the examiner's evaluation of the candidate's performance and they are liable to affect the candidate.[37] This reasoning would apply by analogy to an article submitted for peer review and the comments of the reviewer. Despite the fact that publishers tend to refer to this process as anonymous, suggesting it would fall outside the law's scope, we would therefore conclude that the peer review process constitutes personal data processing to which the data protection framework applies.

A further example is the act of uploading some content to social media, for instance, a photograph with friends or a video of colleagues. This would again easily meet the threshold criteria for the law to apply. Personal data can be *any* information: it is not restricted to information that is private or sensitive.[38] This information is linked to them in terms of its content: it is about them and the processing of this information might impact upon them, for instance, if they were photographed with friends during the working day. Even if they could not be immediately identified on the basis of the photograph, they are identifiable at least

[33] Case C-434/16, *Nowak v Data Protection Commissioner* EU:C:2017:994, para 34. One might argue that the article itself is simply data—a source of information—that needs to be read to reveal information about the individual, however, the Court has not, as of yet, made this distinction between data and information.
[34] *Durant v Financial Services Authority* [2003] EWCA Civ 1746.
[35] *Nowak* (n 33) para 35.
[36] ibid, paras 37–39.
[37] ibid, para 43.
[38] ibid, para 34.

to the person who uploaded the content online. Notably, they are also potentially identifiable to third parties such as phone companies if, using means likely reasonably to be used, they could combine this data with other data they hold, such as geo-location data, to identify the individuals concerned.[39] Here one might object that the social media user has a right to impart information as part of their right to freedom of expression, thus excluding the data protection rules. However, rather than excluding protected free speech from the scope of data protection law, it is brought within the scope of the data protection framework and tensions between data protection and freedom of expression are reconciled from within the data protection framework.[40] This is similar to the example provided by Advocate General Bobek in his Opinion in *X and Z*: an individual in a pub who shares an e-mail containing an unflattering remark about a neighbour with a few friends becomes a data controller subject to the GDPR's obligations. At the hearing in that case, the Advocate General noted that the Commission accepted that even the incidental processing of personal data triggers the GDPR's rights and obligations and that it had difficulty explaining where the limits of the law lie.[41]

At its more extreme, the literature provides examples of data which can plausibly be argued to meet the definition of personal data although intuitively 'far from being "personal"'.[42] Purtova takes the example of a smart city project in the Dutch city of Eindhoven initiated by a public–private collective to anticipate, prevent or de-escalate anti-social behaviour on Stratumseind, a street known for its social life. The data used for this behavioural regulation is gathered from multiple sources and includes weather data, such as rainfall per hour and wind direction and speed. Purtova reasons that weather contains information which is then datafied; that this relates to individuals as it can be used to assess and influence behaviour deemed undesirable and that this information, when combined with other data collected via sensors, can lead to the

[39] Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779 para 43 confirms that it is not necessary that the information enabling identification be in the hands of one entity. However, for such data to constitute identifiable information it must also be assessed whether the data combination is a means reasonably likely to be used to identify an individual (para 45).

[40] See, for instance, Articles 17(4) and 85 GDPR. The balancing of data protection and related rights and freedom of expression must therefore occur within the data protection framework.

[41] Case C-245/20, *X, Z v Autoriteit Persoonsgegevens,* Opinion of AG Bobek (n 9) paras 56 and 57.

[42] Purtova, 'The Law of Everything' (n 9) 57.

identification of individuals. Indeed, this is the very purpose of the Stratumseind 2.0 project. She proposes that weather data could therefore be classified as personal data. Others have applied similar analysis to other environmental artefacts, such as wastewater.[43] Once we start to look around us to apply this definition we see that almost all data is potentially personal data if applied to evaluate or influence individuals thus making data protection the law of everything (or almost everything).

This development is desirable if we consider that it is no longer simply data *about* an individual that might be leveraged to impact upon their rights.[44] Take, for instance, synthetic or artificial data derived from personal or non-personal data to create replica datasets. Such synthetic data may be used to make significant and impactful decisions about identified individuals. In such circumstances, it could be classified as personal data under the GDPR.[45] While this might seem to confirm Purtova's concerns that data protection law is the law of everything, Dalla Corte highlights that information that relates to someone as a result of its impact on them will not necessarily be personal throughout its entire lifecycle.[46] For instance, data about the performance of a vehicle is non-personal data until the point when it relates to someone, such as when it is used to evaluate a driver's performance.[47]

A further feature of the legal framework is that while 'personal data processing' is potentially all encompassing, the limited derogations to the material scope of the GDPR are construed restrictively. Data processing for EU external action, national security purposes and processing by competent authorities for law enforcement purposes fall outside of the GDPR's ambit,[48] as does data processing undertaken by the EU institutions.[49] The only other derogation is for data processing for 'purely personal or household purposes'.[50] The uploading of content to

[43] Bart van der Sloot, 'Truth from the Sewage: Are We Flushing Privacy Down the Drain?' (2021) 12 *European Journal of Law and Technology* https://ejlt.org/index.php/ejlt/article/view/766

[44] Salóme Viljoen, 'A Relational Theory of Data Governance' (2021) 131 Yale L J 573.

[45] Michal S. Gal and Orla Lynskey, 'Synthetic Data: Legal Implications of the Data-Generation Revolution' (forthcoming) *Iowa Law Review* 2023; LSE Legal Studies Working Paper No. 6/2023.

[46] Lorenzo Dalla Corte, 'Scoping Personal Data: Towards a Nuanced Interpretation of the Material Scope of EU Data Protection Law' (2019) 10 *European Journal of Law and Technology* https://ejlt.org/index.php/ejlt/article/view/672.

[47] ibid, 11.

[48] Article 2(2)(b), (a) and (d) GDPR, respectively.

[49] Article 2(3) GDPR.

[50] Article 2(2)(c) GDPR.

social media might seem to constitute such a purpose, however, this is not necessarily so as the *Lindqvist* case demonstrates. Mrs Lindqvist was a church catechist in Sweden who, as coursework for an evening class on computer processing, uploaded short descriptions of her colleagues to the church website. She was criminally prosecuted for illegal data processing and, amongst the many defences invoked in the ensuing court proceedings, was that Mrs Lindqvist was engaged in 'purely personal or household' processing. The CJEU acknowledged that Mrs Lindqvist's activities were charitable and religious rather than commercial[51] but refused to apply this derogation. It considered that the information concerned was 'clearly not' carried out in the course of an activity relating to the private or family life of individuals as the internet publication resulted in the data being made accessible to 'an indefinite number of people'.[52] In later jurisprudence, the Court found that when a home security camera used for personal security captures not only the home but the public footpath outside, it too cannot benefit from this derogation.[53] In this way, many of the routine data processing operations of individuals are brought within the law's fold.

As this section suggests, the concept of personal data has the capacity to bring all impacts of data usage on the fundamental rights of individuals within the remit of data protection law. Given that the law is concerned with the protection of rights rather than the protection of data per se, this expansion is desirable and legitimate. For instance, at the point at which weather data is used to assess an individual's potential criminality, it is appropriate that legal protections are activated. However, as Mrs Lindqvist's case suggests, this does raise questions about to whom the law applies and the extent of their obligations under the framework. It is these questions of scope that require further consideration and to which we shall now turn.

B. *Applied to Everyone? The Data Controller and Joint Controllership*

To whom does this vast legal framework apply? Data protection law distinguishes between data subjects, the individuals whose personal data are processed, and data controllers and processors, who initiate and undertake the data processing. Data controllers act as the 'intellectual

[51] Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, para 39.
[52] ibid, para 47.
[53] Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů* EU:C:2014:2428.

lead'[54] or brains behind the data processing operation—determining the purposes and means of processing[55]—while data processors act as the brawn—conducting the data processing under the instruction of the data controller.[56] Primary legal responsibility is attributed to the data controller, although the GDPR does confer specific responsibilities on the data processor for some tasks.[57]

While these concepts and the division of labour between them appear clear, already in 2010 it was noted that their concrete application was becoming increasingly complex leading to uncertainty regarding responsibilities under the framework.[58] The main reason for this complexity is that modern data processing is itself complex[59]: unlike the conditions that prevailed when data protection laws were first adopted, control over processing is no longer centralised[60] or exercised by singular actors who use available technologies for easily distinguishable purposes.[61] Moreover, technologies confound the distinction between means and ends that the GDPR deploys: determining the appropriate technical tools for the job (de facto a task often assumed by the processor) can have a significant bearing on the purposes to which those tools can be put and, ultimately, the functioning of a socio-technical system.

This messiness of the socio-technical environment is recognised, to some extent, through the concept of joint controllership: controllers can determine the purposes and means of processing alone or 'jointly

[54] Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor"' WP169, adopted on 16 February 2010, 25. This Opinion was superseded by European Data Protection Board (EDPB) Guidelines. EDPB, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' version 1.0, adopted on 2 September 2020, 8.

[55] Article 4(7) GDPR.

[56] Article 4(8) GDPR.

[57] For instance, the processor is under a general obligation to ensure that appropriate technical and organisational measures are in place to ensure the processing complies with the Regulation and that any sub-processors it engages comply with the terms of the original contract with the controller (Article 28 GDPR).

[58] Opinion 1/2010 (n 54) 2.

[59] René Mahieu, Joris van Hoboken and Hadi Asghari, 'Responsibility for Data Protection in a Networked World on the Question of the Controller, "Effective and Complete Protection" and its Application to Data Access Rights in Europe' (2019) 10 *Journal of Intellectual Property*, Information Technology and Electronic Commerce Law 85, 87.

[60] Heleen Janssen, Jennifer Cobbe, Chris Norval and Jatinder Singh, 'Decentralized Data Processing: Personal Data Stores and the GDPR' (2020) 10 *International Data Privacy Law* 356.

[61] Brendan Van Alsenoy, 'Allocating Responsibility among Controllers, Processors, and "Everything in Between": The Definition of Actors and Roles in Directive 95/46/EC' (2012) *Computer Law & Security Review* 25, 27.

with others'. This joint control can take different forms: it can result from a common decision on purposes and means or from 'converging decisions', where complementary decisions have a tangible impact on the purposes and means of processing and the processing would not be possible without the participation of the jointly controlling entities.[62] For our purposes, what is significant is that the concept of controllership is both defined and interpreted expansively. Per the definition, a controller or a joint controller can be a 'natural or legal person, public authority, agency or any other body'.[63] Like other forms of regulation, such as environmental regulation and consumer protection laws, data protection is a form of mixed-economy oversight: the law, therefore, applies equally to public actors, such as local authorities or departments of government, as it does to private enterprise. For the latter, there is little differentiation made between large multinational companies and the local corner shop.[64] Moreover, the law brings individuals within its reach as data controllers, subject to the limited derogation for purely personal and household processing noted above.

The CJEU has had opportunity to interpret the notion of controllership on numerous occasions, taking these opportunities to stretch the concept to ensure the 'complete and effective' protection of individuals. We could locate the foundations for this broad approach in the Court's *Google Spain* judgement. While this ruling is best known for its recognition of a 'right to be forgotten' in EU data protection law, its finding that Google search engine is a data controller was also momentous.[65] Notably, in an earlier advisory opinion on the application of data protection law to search engines, the advisory body comprised of data protection regulators (the Article 29 Working Party) had considered that where a search engine acts purely as an intermediary, the principle of

[62] EDPB Guidelines (n 54) 3 and 19.

[63] Article 4(7) GDPR. Data controllers and data processors also benefit from procedural rights, such as the right to lodge a complaint with a supervisory authority: Article 77(1) GDPR.

[64] The GDPR does recognise the specific needs of micro, small- and medium-sized enterprises to some extent in several recitals (recitals 13, 98, 137 and 167). It provides that their specific needs should be taken into account when codes of conduct are drawn up to contribute to the Regulation's proper application and when certification measures are introduced, although neither codes of conduct nor certification have been widely adopted so far (Articles 40 and 42 GDPR).

[65] The jurisdictional component of this case was also notable. The Court had held that although Google Inc., the parent company responsible for the coordination of Google's data processing operations was established in the USA, the presence of a subsidiary in Spain selling advertising to cross-subsidise these operations was sufficient to bring the processing within the scope of EU data protection law. *Google Spain* (n 2) para 55.

proportionality requires that it should not be considered the principal controller of the content.[66] However, the Court implicitly rejected analogies with other areas of law where intermediaries such as Google Search enjoy quasi-immunity from liability for hosting illegal content until they have actual or constructive awareness of such content. Google had argued that when providing hyperlinks to content already available online it did not differentiate between links to primary publications containing personal data and those that did not.[67] The Court applied the controllership test broadly, finding that in the context of this linking activity it is the search engine operator that determines the purposes and means of the personal data processing.[68] It considered that it would be contrary to the clear wording of the definition of data controller and its objective to exclude search engine operators, going on to note that the role of search engine operators is distinct from primary publishers and that the former is liable to affect fundamental rights to privacy and data protection 'significantly and additionally' compared with the latter.[69] Importantly, the Court considered that the objective of the broad definition of data controller is to ensure 'effective and complete protection of data subjects'.[70]

Later jurisprudence brought this concern for the 'effective and complete' protection of individuals to the fore, sometimes at the expense of the law's literal meaning.[71] In *Wirtschaftsakademie* (*Facebook fan pages)* the Court held that the administrator of a fan page on Facebook was a joint controller.[72] Visitors to the fan page, both Facebook users and non-users alike, had data collecting cookies placed on their devices by Facebook and the Court reasoned that the fan page operator provided Facebook with this opportunity.[73] Moreover, the fan page operator also defined the parameters for the statistical analysis of visitor's data conducted

[66] Article 29 Working Party, 'Opinion 1/2008 on data protection issues related to search engines', adopted on 4 April 2008 WP148, 14.

[67] *Google Spain* (n 2) para 22.

[68] ibid, para 33.

[69] ibid, paras 34 and 38.

[70] ibid, para 34.

[71] Mahieu and von Hoboken note that the Court is more concerned with ensuring effective and complete protection 'than a more literal interpretation of the law's text would seem to point to'. René Mahieu and Joris von Hoboken, 'Fashion ID: Introducing a Phase-oriented Approach to Data Protection?' (*European Law Blog*, 30 September 2019).

[72] Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (Facebook fan pages)* ECLI:EU:C:2018:388, para 39.

[73] ibid, para 35.

by Facebook, thereby contributing to and determining the purposes and means of processing.[74] The later *Fashion ID* case, where the Court considered whether the integration of a Facebook social plug-in (the Facebook like button) into a website was sufficient to make the website operator a joint controller, confirmed that the definition of parameters for data analytics by a Facebook fan page was not what was decisive.[75] In *Fashion ID*, the mere presence of the piece of Facebook code on the website—triggered when the website was consulted—was sufficient to transmit data from the website user's device to Facebook. The website visitor did not need to click on the plug-in or be a Facebook user for this to occur.[76] The Court was asked whether embedding a piece of Facebook code on a website was sufficient for the website operator to constitute a data controller, particularly given that once the data was transmitted to Facebook the website operator had no influence on the subsequent data processing. The Court broke the data processing operations down into segments. It determined that Fashion ID exercised joint control over the collection and transmission of the personal data of visitors to its website, a first segment, however, it was not responsible for subsequent processing operations, over which it had no influence.[77] Specifically with reference to the means of processing, the Court emphasised that Fashion ID was 'fully aware' of the fact that the embedded plug-in served as a tool for the collection and transmission of personal data to Facebook.[78] The Court concluded that through the embedding of the plug-in on its website, Fashion ID exerted 'decisive influence' over the data processing that would not have occurred in the absence of the plugin[79] and that there was joint control over the data processing operation.[80] In support of this conclusion, the Court pointed to the mutual benefit the data processing provided to Fashion ID and Facebook Ireland.[81]

[74] ibid, para 36.

[75] This was a reasonable assumption based on the way in which the Court set out its reasoning. For instance, Mahieu et al (n 59, 94) were critical of the Court's decision in *Facebook fan pages* stating that 'it seems unreasonable that if Facebook would not offer the so-called Insights function, the fan page administrator would no longer have responsibility for the data processing'.

[76] Case C-40/17, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* ECLI:EU:C:2019:629, para 75.

[77] ibid, para 76. The Court noted that it seemed 'impossible' that Fashion ID determines the purposes and means of these subsequent processing operations.

[78] ibid, para 77.

[79] ibid, para 78.

[80] ibid, para 79.

[81] ibid, para 80.

In both of these instances, the fan pages and website operators did not 'hold' or have access to the data undergoing processing, thus rendering them incapable of complying with the vast majority of the regulatory framework (a point to which we shall return). The Court addresses this point, finding that the classification of data controller does not necessitate that the data controller has access itself to the personal data collected and transmitted.[82] Implicitly, the role of facilitating and benefiting from data processing is sufficient to incur legal responsibility.[83] *Jehovan todistajat* offers more explicit confirmation of this understanding of controllership in the context of the relationship between the Jehovah's witness community, its congregations and its preaching members.[84] In the conduct of their preaching activities, preaching members of the Jehovah's witness community (the community) took notes regarding the people they met. These notes served the dual purpose of acting as an aid for future visits and to compile a 'refusal register' of those who did not want to be contacted again. The community and its congregations coordinated this preaching activity by creating maps allowing for the allocation of areas between preaching members and keeping records about preachers and the number of leaflets they distributed.[85] While the preaching members received written guidelines on note-taking published in a magazine for members, they exercised their discretion as to the circumstances in which they should collect data; which data to collect; and how those data are subsequently processed.[86] Yet, the role of the community in 'organising, coordinating and encouraging' this preaching activity was sufficient for it to be deemed a joint controller.[87]

In *Jehovan*, we might distinguish between the overarching aim or purpose of data processing—to encourage new members to join the community—which is determined by the community and more essential elements of the processing (such as which data to be processed and who should have access to the data) which was determined by the preaching members.[88] The orchestrating role of the community is sufficient to

[82] ibid, para 82. *Facebook fan pages* (n 72) para 38.

[83] This was noted by the Advocate General in *Fashion ID* who considered that taken to extremes this makes anyone in a 'personal data chain' who makes data processing possible a controller. Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* ECLI:EU:C:2019:629, Opinion of AG Bobek, para 74.

[84] Case C-25/17, Jehovan todistajat EU:C:2018:551.

[85] ibid, para 16.

[86] ibid, para 23.

[87] ibid, para 73.

[88] The EDPB distinguishes between essential means of processing (which is closely linked to purposes) and includes determining what and whose personal data is processed and for long, and non-essential means which concerns more practical aspects of implementation (e.g. Hardware choices). EDPB Guidelines (n 54) 14.

establish responsibility under data protection law, without the need for access to the data[89] or to have produced written guidelines around data processing.[90] This is perhaps unsurprising given that the preaching was carried out in furtherance of the overarching objectives of the community—to spread its faith—and the community acted as the 'intellectual lead' on the data processing. In a subsequent case, the Court is asked to determine whether a standard-setting organisation that offers its members a standard for managing consent specifying how personal data is stored and disseminated is a data controller.[91] The way in which the standard-setting organisation 'organises and coordinates' personal data processing through this standard seems highly likely to meet the criteria set by the Court in *Jehovan*.

This low legal threshold for controllership, when combined with technical–organisational developments, particularly the increasingly interconnected nature of information systems and markets, will therefore make joint controllership more prevalent.[92] This has the benefit of enabling regulators to more easily bring complex data processing structures within their regulatory remits, as was the case in the standard-setting investigation noted above. However, it also brings more individuals and tangential actors within the law's fold. We might conclude that, to the extent that it is necessary to establish 'which level of influence on the "why" and "how" should entail the qualification of an entity as a controller',[93] the answer is very little. This caselaw leaves one with the impression that everyone is responsible for data processing from the facilitators (such as Fashion ID) to the orchestrators (such as the community). Data protection is, it seems, the law of everything applied to everyone. We will return to the question of whether this is desirable below.

C. *Failed Attempts to Limit the Law*

This expansive evolution of the scope of data protection law has been challenged. Prior to the development of European case law, British courts tended to interpret its material scope more restrictively. The notion of

[89] *Jehovan* (n 84) para 69.
[90] ibid, para 67.
[91] C-604/22, *IAB Europe v Gegevensbeschermingsautoriteit* (application pending).
[92] Lee A. Bygrave and Luca Tosoni, 'Article 4(7): Controller' in Christopher Kuner, Lee A Bygrave, Christopher Docksey and Laura Drechsler (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 145, 152.
[93] EDPB Guidelines (n 54) 13.

processing was interpreted narrowly to exclude the act of anonymising personal data on the grounds of 'common sense and justice alike'[94] while information only constituted personal data relating to someone when it was private or biographical in a significant sense.[95] At European level, pushback has come from within the Court in the Opinions of its Advocates General.

Advocate General Sharpston sought to keep the material scope of the rules in check by proposing alternative readings of the concepts of automation, processing and personal data in her Opinions. It is recalled that the GDPR applies to personal data that is processed manually as part of a filing system or that is processed 'wholly or partly by automated means'. In an early case where the right to access documents was pitted against the data protection rights of those featuring in the documents, she sought to avoid a balancing of interests by suggesting that the data protection rules did not apply. The retention and making available of these meeting minutes using a search function was not, she opined, 'automated' processing. Her reasoning was that throughout this process the 'individual human element plays such a preponderant part and retains control'[96] in contrast to 'intrinsically automated' processing operations such as the loading of a website. The search function, like the use of an electric drill, could be replicated by humans but simply with less efficiency.[97] This reasoning was undoubtedly influenced by the Advocate General's opinion that 'the essence of what is being stored is the record of each meeting, not the incidental personal data to be found in the names of the attendees'.[98] Had the Advocate General's reasoning been accepted, the range of processing operations to which the data protection framework would apply would have been dramatically limited.[99] The Court did not follow, or even acknowledge, the Advocate

[94] *R v Department of Health; ex parte Source Informatics Ltd* [2000] 1 All ER 786, para 799. In *R v Department of Health* the UK Court of Appeal held obiter dicta that the process of anonymising personal data did not qualify as a form of 'processing' under the 1998 DPA.

[95] *Durant* (n 34).

[96] Case C-28/08P, *European Commission v The Bavarian Lager Co. Ltd* ECLI:EU:C:2009:624, Opinion of AG Sharpston, paras 144–146.

[97] ibid, para 146.

[98] ibid, paras 137 and 139.

[99] It is perhaps also notable that the Advocate General took a holistic approach to 'processing' viewing the processing operation as a composite whole: the she looked at the overall process of retrieving a legally contested digital document as opposed to a series of smaller, distinct processing operations.

General's attempt to place boundaries around the notion of personal data processing.[100]

When the Court was asked to consider whether the legal analysis found in an administrative note concerning the immigration status of several individuals constituted personal data in the *YS, M and S* case, Advocate General Sharpston again proposed to restrict the law's material scope. As in *Bavarian Lager* she emphasised the human dimension of the processing. Legal analysis is a process controlled entirely by individual human intervention through which personal data (in so far as they are relevant to the legal analysis) are assessed, classified in legal terms and subjected to the application of the law, and by which a decision is taken on a question of law.[101] Once again, the Court did not acknowledge this perspective. It did, however, find her opinion on what constitutes personal data more persuasive. Her opinion suggested that the definition of personal data should be confined to 'facts' about an individual, whether objective (e.g. weight in kilos) or subjective (underweight or overweight),[102] to the exclusion of the reasoning or explanation used to reach such conclusions or facts.[103] She was unconvinced that the definition of personal data should 'be read so widely as to cover all of the communicable content in which factual elements relating to a data subject are embedded'.[104]

The Court concurred finding that legal analysis is not information relating to the applicant but is, at most, information about the assessment and application of the law to the applicant's situation.[105] Like the Advocate General, it supported this conclusion by reference to the broader legal framework, suggesting that its interpretation was borne out by its objectives and general scheme.[106] It reasoned that in order to promote the law's objectives of protecting fundamental rights, including privacy, the law gives individuals the right to access data to conduct

[100] Instead, the Court simply endorsed the General Court's finding that the 'communication of data, by transmission, dissemination or otherwise making available, falls within the definition of processing'. Case C-28/08P *European Commission v The Bavarian Lager Co. Ltd* [2010] ECR I-06055, para 69; endorsing [105] in T-194/04 *The Bavarian Lager Co. Ltd v Commission* [2007] ECR II-04523.

[101] Case C-141/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* ECLI:EU:C:2020:753, Opinion of AG Sharpston, para 63.

[102] ibid, para 56.

[103] ibid, paras 58 and 59.

[104] ibid, paras 55.

[105] Case C-141/12 *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S* ECLI:EU:C:2020:753, para 40.

[106] ibid, para 41.

'necessary checks' (to check its legality; to rectify or delete in some circumstances). In this instance, as the legal analysis itself is not liable to be subject to the checks set out in the right to access, such as an accuracy check, granting access to the data would not serve the law's purpose.[107] The Court's reasoning in this case is flawed: it rendered the scope of application of the legal framework contingent on whether substantive rights can be exercised in a particular scenario although the scope of the legal framework is a logically prior question.[108] What is notable, however, is that YS is a 'rare instance in which the Court has read the concept of "personal data" restrictively'.[109]

However, in the later *Nowak* case, the Court seems to recognise this misstep as it differentiates explicitly between 'classification'—the scope of the rules—and 'consequences'—the substantive responsibilities they impose. It held that whether the answers and exam comments could be classified as personal data should not be affected by the consequences of that classification.[110] To confirm this point, the Court emphasised that if data are not personal data they are entirely excluded from data protection's principles, safeguards and rights.[111] While the Court made a weak reference to *YS and M and S*, intimating that it might be distinguished on the facts, its findings and reasoning in *Nowak* stand in opposition to *YS*. At best, the current status of *YS* is 'somewhat uncertain'.[112] However, given the Court's later expansive line in *Nowak*, it is perhaps more reasonable to treat *YS* as an anomaly.

The scope of the notion of controllership has also been subject to contestation. In *Facebook fan pages*, the referring court hinted at the possibility of a 'third way' to attribute responsibility for data processing beyond controllership and joint controllership. It considered that the operator of a fan page was not a controller but queried whether the action of choosing which operators to engage with should entail some responsibility for the fan page host.[113] The Court simply considered the

[107] ibid, paras 42–46.

[108] Orla Lynskey, 'Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing' (2019) 15 *International Journal of Law in Context* 162, 169. This finding was likely influenced by a desire to avoid undermining established principles of administrative law, like freedom of information, in Member States.

[109] Lee A. Bygrave and Luca Tosoni, 'Article 4(1): Personal Data' in Christopher Kuner, Lee A Bygrave, Christopher Docksey and Laura Drechsler (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 103, 110.

[110] *Nowak* (n 33) para 46.

[111] ibid, para 49.

[112] Bygrave and Tosoni, 'Article 4(1)' (n 109) 110.

[113] *Facebook fan pages* (n 72) para 24(1).

fan page operator to be a joint controller. In their opinions on data controllership, Advocates General also expressed their unease about the expansive personal scope of the law, albeit without fully articulating their concerns. In *Google Spain*, the Advocate General proposed a knowledge component to controllership[114]: the data controller should be aware in some 'semantically relevant way' of what kind of personal data they are processing and why[115] and then process this data 'with some intention which relates to their processing *as* personal data'.[116] Advocate General Bobek was most forthright in expressing his concerns, openly querying whether this strategy of broadly interpreting controllership—making 'everyone' responsible—would enhance effective protection.[117] The Court was not 'faced with the practical implications of such a sweeping definitional approach'.[118] The Advocate General does not, however, develop how the broad scope of the law might hinder its effectiveness or what the practical implications of this broad scope might be. Having shown how judicial developments in the EU mean that data protection law might not be credibly classified as the law of everything applied to everyone, we now turn to examining this question: what are the consequences of this broad scope for the effectiveness of the law.

3. *Meaningless Law on the Books? The Tension between Complete and Effective Protection*

The scope of data protection law has been interpreted expansively with a view to preventing human rights infringements. To achieve their preventive function, Simitis argued that these rules should be strictly applied but, primarily, that they adapt to 'both the exigencies of an evolving technology and of the varying structural as well as organisational particularities of the different controllers'.[119] No doubt the Court considers that it has

[114] This aligns to the findings of the Supreme Court of Milan which held that as long as the illicit data is unknown to the service provider it cannot be a data controller. Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge Studies in European Law and Policy, CUP 2022), 138.

[115] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* EU:C:2014:317, Opinion of AG Jääskinen, para 83

[116] ibid, para 82.

[117] Case C-40/17, *Fashion ID*, Opinion of AG Bobek (n 83), para 71.

[118] ibid, para 72.

[119] Spiros Simitis, 'Legal and Political Context of the Protection of Personal Data and Privacy' (Speech in Montreal, September 1997) Council of Europe Archives (T-PD (97) 17—on file with the author), 7.

remained true to this mission in its jurisprudence. However, this approach is increasingly questioned. Advocate General Bobek suggests that the current approach is 'gradually transforming the GDPR into one of the most de facto disregarded legislative frameworks under EU law'.[120] Similar reservations are expressed in the academic literature. Bygrave and Tosoni note that the law's enormous scope of application is 'perhaps beyond what it can cope with in terms of actual compliance and enforcement'.[121] Nolan observes that the Court's approach appears to assume that 'by applying data protection law to more actors better protective outcomes will be achieved'[122] while Koops more explicitly declares data protection law to be 'meaningless law on the books' as a result of, amongst others, its broad scope.[123] Therefore although the Court justifies its expansive application of the law on human rights grounds, this quest for completeness may be in tension with the law's effectiveness and the attainment of these human rights objectives. In other words, we must query whether data protection law can be both complete *and* effective.

A. *Assessing the Effectiveness of the Law*

When we test this claim—that data protection law can be all encompassing or effective but not both—we are immediately faced with the challenge of determining appropriate parameters to assess the effectiveness of the law. As one data protection authority has noted, while the volume of work they undertake is ever intensifying, what remains elusive 'is any agreed standard by which to measure the impacts and success or otherwise of a regulatory intervention in the form of GDPR that applies to literally everything'.[124] While the idea of measuring the impact of human rights and the methodologies used remain contested, scholars such as De Búrca have sought to break the deadlock by proposing an experimentalist account of human rights to assess their effectiveness.[125] However, such accounts speak predominantly to how Treaty and Charter rights, rather than the legislative frameworks that implement them, have been harnessed for social change. Policymakers, journalists

[120] Case C-245/20, *X, Z v Autoriteit Persoonsgegevens,* Opinion of AG Bobek (n 9) para 65.

[121] Bygrave and Tosoni, 'Article 4(1): Personal Data' (n 109) 113. We will return to the distinction between compliance and enforcement below.

[122] Katherine Nolan. *The Individual in EU Data Protection Law* (PhD thesis; LSE Law School), 130.

[123] Koops (n 9) 251.

[124] Irish Data Protection Commission, 'Annual Report 2021', 5.

[125] Gráinne de Búrca, *Reframing Human Rights in a Turbulent Era* (OUP 2021), 46.

and civil society organisations tend to speak of the effectiveness of the GDPR in terms of the complaints resolved by authorities and the remedies and sanctions imposed.[126] The number of complaints lodged by data subjects was also deemed by the European Commission to be an appropriate indicator of the impact of the GDPR to be taken into consideration when monitoring the implementation of the law.[127] However, the number of complaints alone provide an inconclusive indication of success. Not only is data gathering in this area very inconsistent, detracting from its reliability[128] but, more fundamentally, interpreting this data is difficult. A low number of complaints or insignificant fines could be indicative of either a dysfunctional system of enforcement or widespread compliance with existing obligations.[129] Equally, while by August 2023 an impressive 1.4 million requests for the erasure of links from Google's search engine have been submitted pursuant to GDPR,[130] this figure gives us only a small insight into the overall exercise of individual rights and tells us nothing of who is exercising their rights and whether these requests were appropriately handled.[131] In assessing the effectiveness of the law, we might then return to a simple test that asks what are the law's objectives and queries whether these objectives have successfully been attained.[132]

The stated objectives of the GDPR are two-fold: to remove impediments to the free flow of personal data within the EU and to protect fundamental rights, in particular data protection.[133] These different

[126] Adam Satariano, 'Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates' *New York Times* (27 April 2020), https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe; Johnny Ryan and Alan Toner, 'Europe's Governments are Failing the GDPR' (Brave Report 2020).

[127] Impact Assessment, 'Commission Staff Working Document accompanying SEC(2012) 72 final', *Brussels* (2 January 2012), 103.

[128] Access Now, 'The right to lodge a data protection complaint: OK, but then what? An empirical study of current practices under the GDPR', June 2022. More generally, it noted that 'there is a lack of precise information on complaint-handling, including on the number of complaints lodged with DPAs' (ibid, 4).

[129] The number of complaints received could also be an indicator of the relevance and visibility of the law to individuals.

[130] Google Transparency Report, 'Requests to Delist Content Under European Privacy Law', https://transparencyreport.google.com/eu-privacy/overview?hl=en-GB.

[131] Julia Powles, 'The Case That Won't Be Forgotten' (2015) 47 Loy U Chi LJ 583. See also, Julia Powles and Enrique Chaparro, 'How Google Determined Our Right to Be Forgotten', *The Guardian* (18 February 2015).

[132] Julia Black, *Rules and Regulators* (OUP 1997), 9.

[133] Article 1(2) and (3) GDPR. Chapter V GDPR subjects data flows to outside the EU to distinct legal requirements to ensure that the level of protection individuals receive when the data is transferred out of the EU is 'essentially equivalent' to within the EU to prevent the circumvention of the data protection framework.

ambitions of data protection are often not mutually exclusive and are sometimes in tension.[134] The GDPR's fundamental rights objective has become dominant in its interpretation in recent years.[135] However, parsing this fundamental rights objective further, we can see that the content of the right to data protection itself remains contested. The right has been characterised in different ways: as promoting individual control over personal data; ensuring 'fair' processing of personal data; a right which simply guarantees legislative safeguards for data processing; and as instrumental for other rights.[136] Moreover, the Court has explicitly acknowledged that not all violations of the GDPR entail a fundamental rights interference,[137] thereby confirming that there are provisions of the law that do not have a fundamental rights character.

Whether the law is successful in achieving the protection of fundamental rights, in particular data protection, may differ depending on which of these conceptualisations of data protection one prefers. However, for simplicity, assuming that the GDPR gives at least partial expression to the right to data protection,[138] we might then infer that compliance with the GDPR would itself achieve the law's objective of fundamental rights protection. This vision of effectiveness equates legal compliance with

[134] Macenaite, for instance, considers the aims of developing a data-driven economy and protecting fundamental rights and freedoms to be essentially contradictory while Yakovleva envisages their reconciliation. Milda Macenaite, 'The "Riskification" of European Data Protection Law through a Two-Fold Shift' (2017) 8 *European Journal of Risk Regulation* 506, 507; Svetlana Yakovleva, 'Personal Data Transfers in International Trade and EU Law: A Tale of Two Necessities' (2020) 21 *Journal of World Investment & Trade* 881, 888.

[135] Kristina Irion, 'A Special Regard: The Court of Justice and the Fundamental Rights to Privacy and Data Protection' in Ulrich Faber et al (eds), *Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte* (Nomos 2016) 873. This was foreseen by Spiros Simitis, 'From the Market to the Polis: The EU Directive on the Protection of Personal Data' (1994–1995) 80 *Iowa Law Review* 445.

[136] Plixavra Vogiatzoglou and Peggy Valcke, 'Two Decades of Article 8 CFR: A Critical Exploration of the Fundamental Right to Personal Data Protection in EU Law' in Eleni Kosta, Ronald Leenes and Irene Kamara (eds), *Research Handbook on EU data protection* (Edward Elgar 2022). See also, Gonzalez Fuster and Hijmans (n 3).

[137] C-60/22, *UZ v Bundesrepublik Deutschland* ECLI:EU:C:2023:373, para 65.

[138] The Court has not explicitly confirmed that the GDPR 'gives expression' to the right to data protection, which might result in a self-referential system whereby the right to data protection is interpreted in light of secondary law. Nadezhda Purtova, 'Default Entitlements in Personal Data in the Proposed Regulation: Informational Self-determination Off the Table … and Back On Again?' (2014) 30 *Computer Law & Security Review* 6, 11.

success. This assumes that the legal rules are the 'right' ones to achieve the objectives of data protection laws. In other words, by achieving high levels of compliance we would achieve the law's objectives of fundamental rights protection. However, existing legal scholarship appears to challenge this assumption. Bygrave, for instance, observes a paradox in the enactment of 'increasingly elaborate legal structures' for privacy while privacy protection is increasingly eroded.[139] Richards similarly queries why people are so concerned about the Death of Privacy when there is so much privacy law.[140] There is also some limited empirical evidence to suggest that modern data protection frameworks encourage 'symbolic compliance' by allowing the information industry to apply the law in a way that aligns to corporate rather than public objectives.[141] While this empirical work was conducted in the USA, its findings are also said to reflect on the GDPR. Further empirical research is required to assess how the law is being received on the ground. early evidence suggests that rather than even encouraging symbolic compliance there remains widespread non-compliance with the law in reality. Writing in 2022 Lancieri examined the 26 independent empirical studies to assess the impact of the GDPR and the California Consumer Protection Act on legal compliance and concluded that non-compliance remains widespread.[142] Such non-compliance includes obvious violations, for instance, that 85% of Europe's most accessed websites continued to track users even after they had opted out of such tracking.[143] Thus while compliance requirements will undoubtedly play an important role in securing the application of the GDPR,[144] this suggests that over-reliance on controller compliance

[139] This echoes Koops' earlier observation that 'we see data protection bodies moving all around, but they do not provide us with real protection'. Koops (n 9) 259.

[140] Neil Richards, *Why Privacy Matters* (OUP 2022) 52.

[141] Ari Ezra Waldman, *Industry Unbound: The Inside Story of Privacy, Data and Corporate Power* (CUP 2021), 114. This echoes the findings of Black in the field of financial services regulation where she refers to 'creative compliance'. Julia Black, 'Learning from Failures: "New Governance" Techniques and the Financial Crisis' (2012) 75 *Modern Law Review* 1037.

[142] Filippo Lancieri, 'Narrowing Data Protection's Enforcement Gap' (2022) 74 *Maine Law Review* 15, Appendix: 65–72.

[143] Lancieri cites Sanchez-Rola et al. to this effect. See, Iskander Sanchez-Rola et al., 'Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control' (2019) *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* 1, 3–5.

[144] Hodges advocates that effective data protection requires 'a system of constructive engagement in resolving problems, involving relationships based on evidence of trust' between regulators and businesses. Christopher Hodges, 'Delivering Data Protection: Trust and Ethical Culture' (2018) 1 *European Data Protection Law Review* 65, 79.

over enforcement would be erroneous.[145] Yet, even where the desire to comply is present, the law's complete scope makes compliance with its provisions impossible in some circumstances (B) while rendering the enforcement needed to complement compliance strategies more challenging for regulators (C). In this way, complete protection is pitted against effective protection.

B. *The Practical Impossibility of Compliance*

It follows from the Court's jurisprudence that the broad scope of responsibility it envisages renders compliance with the law practically impossible in some circumstances, one of Fuller's characteristics of a bad law.[146] The practical impossibility of compliance is best illustrated through the Court's caselaw on joint controllership, discussed above. It follows from this case law that in networked situations, for instance, where a student society uses Facebook to host a fan page, data controller responsibility is segmented. The student society would need to comply with data protection law for any element of the processing that it facilitates while Facebook would need to comply for any data processing operations it undertakes jointly with or independently of the student society. Some provisions of the GDPR apply awkwardly to this situation. For example, the requirement found in Article 26 GDPR which stipulates that joint controllers should arrange between them their respective responsibilities either functions as a legal fiction when applied between big technology platforms and natural persons or is widely disregarded. Both scenarios detract from the law's credibility and legitimacy. However, joint controllership also leads to situations where it will be impossible in practice for the student society to comply with all of its obligations under data protection law. The Court has, for example, held that joint controllership is not contingent on the controllers having access to the data being processed.[147] Without such access the student society cannot comply with requests from individuals in relation to that data (such as data access, rectification or deletion requests). This necessarily raises the question of whether an individual or entity ought to be designated a data controller if they do not have or have not had access to the data that renders them

[145] Hielke Hijmans, 'How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner? A Reaction to Christopher Hodges' (2018) 1 *European Data Protection Law Review* 80, 82.

[146] Fuller refers to 'rules that require conduct beyond the powers of the affected party'. Lon L. Fuller, *The Morality of Law* (Revised edn, Yale University Press 1969), 39.

[147] *Facebook fan pages* (n 72) para 38; *Jehovan* (n 84) para 69.

legally responsible. In principle, as a joint controller the student society or individual could require others to provide such access pursuant to Articles 26 and 28 GDPR. Indeed, companies such as Meta have put in place a contractual addendum indicating that Meta will retain responsibility for compliance with data subjects' rights that necessitate data access.[148] This fills the legal lacuna in this instance but it is noteworthy that this renders the compliance of the student society with the GDPR contingent on Meta's contractual wishes. More broadly, this approach to controllership assumes that cooperation is feasible given the number of entities deemed joint data controllers pursuant to this approach and the often asymmetrical power relations between them. The same can be said for legal requirements that require no data for compliance, such as the GDPR's transparency requirements.[149] Mahieu and Von Hoboken provide the example of the following transparency notice to illustrate this point evocatively:

> We collect your IP address and browser-ID and transfer this personal data to Facebook. We do not know what Facebook does with the data. Click here to proceed.

By segmenting responsibility to ensure complete data protection, key provisions of data protection law are rendered meaningless in the process. The Court had been warned of this consequence by one of its Advocates General who considered that, when it came to controllership, a conceptual lack of clarity upstream about who was responsible for what processing might cross 'into the realm of actually impossibility for a potential joint controller to comply with valid legislation'.[150] This warning did not influence the Court.

The Opinions of the Advocates General in these cases on joint controllership give some insights into the Court's thinking in developing responsibility in this way. The ambition, it seems, was a policy one: that by making more individuals and entities responsible for data protection compliance this would introduce some bottom-up pressure on more significant data controllers to take compliance seriously. This approach has been subsequently vindicated to some extent as it has given data protection regulators more leverage to apply the law to address systemic data protection concerns. For instance, civil society organisation

[148] See https://www.facebook.com//legal/controller_addendum accessed 23 August 2023.
[149] Articles 12–14 GDPR.
[150] Case C-40/17, *Fashion ID*, Opinion of AG Bobek (n 83) para 84.

NOYB submitted 101 complaints to various European data protection authorities arguing that website operators that used Google Analytics and Facebook Business Tools transferred data illegally from the EU to the USA. In its initial advisory assessment of this practice, the European Data Protection Board (EDPB) emphasised that each website operator must 'carefully examine whether the respective tool can be used in compliance with data protection requirements'.[151] Moreover, given the difficulties experienced in the use of the GDPR's pan-European enforcement mechanism (the one-stop-shop),[152] this approach also potentially returns competence to national data protection authorities if the data processing operations of the joint controller affect residents in that State only.[153]

Therefore, while this approach is not without merit, what is overlooked in the equation is that the business models in question co-opt individuals and entities into data processing but without giving them any real stake or meaningful control in the data processing operations. The real locus of power over data processing lies not with the millions of joint controllers who embed such analytics tools in their content and services but with the operators who provide them. One might also wonder how the data subject stands to benefit from the designation of an entity that cannot comply with core data protection rights, such as access and erasure, as a data controller. Joint controllership as conceived by the Court in *Jehovan*, extending responsibilities to those who coordinate and orchestrate data processing operations, appears to more accurately capture the real site of power in digital ecosystems and therefore offers a more effective leverage point for regulatory intervention. Indeed, relying on the *Jehovan* logic, the Belgian regulator has analysed the data processing operations of almost the entire online advertising technology ecosystem by focussing on a critical apex entity, the Interactive Advertising Bureau (IAB).[154] We might be more willing to

[151] EDPB, 'Report of the Work Undertaken by the Supervisory Authorities within the 101 Task Force' (28 March 2023), 10.

[152] There is emerging consensus that there are structural impediments to its effective enforcement. For instance, the European Data Protection Supervisor hosted a conference in May 2022 on data protection enforcement to make progress on this issue. European Data Protection Supervisor, Effective enforcement in the digital world, June 2022. https://www.edpsconference2022.eu/en.

[153] This was the case in *Facebook Fanpages* (n 72).

[154] Michael Veale, Midas Nouwens and Cristiana Teixeira Santos, 'Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the DPA Decision?' (2022) *Technology and Regulation* 12.

accept the practical impossibility of compliance with the law's provisions if it delivers real gains for fundamental rights protection.

C. *Data Protection Authorities as the Regulators of Everything*

Securing effective data protection in Europe will require an appropriate blend of private enforcement (including by civil society actors),[155] compliance by regulated data controllers and public enforcement by regulators. The regulator alone is not responsible for the full application of the law. However, it could be argued that regulators continue to play an out-sized role in the success or failure of the EU data protection regime as the extent to which follow-on private enforcement is initiated or regulatees voluntarily comply with the law is dependent on their actions. It is therefore significant that the law's broad scope of personal application also poses challenges for the regulators tasked with interpreting and enforcing its provisions.

At a very basic level, the volume of cases that regulators deal with has increased significantly since the entry into force of the GDPR, suggesting a 'new level of mobilisation on the part of individuals' to tackle data misuses.[156] For instance, while in 2013 the Irish regulator received 910 complaints between May and December 2018, following the entry into force of the GDPR, it saw this number triple.[157] Regulators report on the number of complaints that they receive annually in their Annual Reports and these figures have been collated on occasion at European level.[158] While this mobilisation is to be welcomed, regulators may lack the capacity to handle the increase in demand for their services. In response to a questionnaire of the EDPB, 82% of regulators explicitly stated that they do not have enough resources to conduct their activities.[159] In this sense, with finite budgets and human resources at their disposal, the broad scope of the law means regulators struggle to fulfil

[155] On the enhancement of the role of civil society actors and public regulators in this space see Lancieri, 'Data Protection's Enforcement Gap' (n 142) 57–60.

[156] Irish Data Protection Commission, 'Annual Report 2018', 5.

[157] ibid, 18.

[158] EDPB, 'Overview on Resources Made Available by Member States to the Data Protection Authorities and on Enforcement Actions by the Data Protection Authorities' (5 August 2021), 10. However, in its study on complaints Access Now notes that what can be gleaned from such figures is limited due to disparities in what is treated as a complaint and the handling of complaints at national level. Access Now (n 128), 4.

[159] ibid, 5. With the exception of Germany which has over 1000 employees, all other regulators had fewer than 300 employees in 2021 (ibid).

their legal supervisory obligations. The solution may lie, in part, with providing regulators with more resources.

Yet, while a lack of resources no doubt exacerbates the enforcement challenge for regulators, the problem may also be one of delimiting appropriate regulatory boundaries when data protection law is applied to everyone. It is not simply the number of regulatees that might complicate the work of regulators but also that the regulated community is extremely diverse. We might contrast this with other areas of regulation, such as energy regulation where the regulator deals primarily with energy firms, or even competition law, where the regulator deals only with 'undertakings' engaged in economic activity.[160] Data protection regulators must regulate, amongst others, the activities of individuals, charities, political parties, public authorities and commercial actors. This diversity of regulatees is significant as regulation—and regulators—benefit from the existence of a 'cohesive interpretive community'. As Black emphasises, for rules to work, that is to apply in a way that would further the overall aims of the regulatory system, the person applying the rule has to 'share the rule maker's interpretation of the rule; they have to belong to the same interpretive community'.[161]

A lack of cohesion amongst regulatees may make a common understanding of the law more difficult to attain resulting in over- or under-compliance. Tales of such compliance misadventures are plentiful in data protection law. In 2019, for example, the Irish regulator needed to reassure publicly the Irish General Post Office that maintaining public bins outside its premises would not violate GDPR.[162] The more diverse the regulated community, the less the regulator will be able to assume some minimum levels of understanding of the rules and the more demanding its task becomes. Moreover, it is apparent that, as a result of the diversity of regulatees under the law, some legal requirements are awkwardly applied to individuals. Not only are many of the

[160] Niamh Dunne, 'Knowing When to See It: State Activities, Economic Activities, and the Concept of Undertaking' (2010) 16 Colum J Eur L 427.

[161] J Black, *Rules and Regulators* (n 132) 30. This is in keeping with later work describing regulation as a 'communicative process'. See, Julia Black, 'Regulatory Conversations', (2002) 29 *Journal of Law and Society* 163, 164.

[162] Ian Begley, 'Office of Data Protection Commissioner Says GPO Can Keep their Bins as Public Litter Is Not in Breach of GDPR rules', *Irish Independent* (2 May 2019). https://www.independent.ie/irish-news/office-of-data-protection-commissioner-says-gpo-can-keep-their-bins-as-public-litter-is-not-in-breach-of-gdpr-rules-38073828.html.

law's requirements predicated on centralised control over a file,[163] but they also assume that a data controller will have certain organisational and bureaucratic capacities at its disposal. The GDPR introduced a wide range of ex ante meta-regulation obligations that apply to controllers, such as the record keeping needed to comply with demonstrable accountability requirements[164] and the requirement to appoint a DPO in some circumstances.[165] As Nolan observes, implicit in these responsibilities is the assumption that controllers are 'commercial, institutional or bureaucratic entities, if controllers are to ever be able to meaningfully comply with their obligations'.[166] While some of these requirements contain exceptions for small- and medium-sized enterprises (and implicitly individuals), this is not universally true.[167] In short, by detracting from common understandings of the law and stretching the application of its requirements to all regulatees, the lack of cohesion in the regulated community can detract from the effectiveness of the law.

The diversity of the regulated community also puts pressure on regulators because they deal with a huge variety of regulatory issues. Recent examples include the systemic issues arising in data-centric industries, such as the ongoing legal investigations into the AdTech industry across Europe[168]; assessing the compliance of public data processing initiatives, such as the use of contact tracing applications at the peak of the Covid-19 pandemic[169]; complaints by individuals about institutional data controllers[170]; and interpersonal complaints, including about the use of

[163] Chris Reed, 'The Law of Unintended Consequences – Embedded Business Models in IT Regulation' (2007) *Journal of Information, Law and Technology* 33, 9 (noting the law's 'implicit assumption that there is central control of personal data processing').

[164] Article 5(2) and 30 GDPR.

[165] Rotem Medzini, 'Credibility in Enhanced Self-regulation: The Case of the European Data Protection Regime' (2021) *Policy & Internet* 13(3) 366.

[166] Nolan (n 122) 37.

[167] Article 30(5) GDPR contains a derogation from the requirement to maintain a record of processing activities for SMEs, however, Article 25 on data protection by design and by default contains no such exceptions.

[168] See, for instance, Autorité de Protection des Données, 'The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR', *Press Release* (2 February 2022); Decision of the litigation chamber, Case number: DOS-2019-01377 (2 February 2022).

[169] EDPB, 'Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak' (21 April 2020); EDPB, 'Guidelines 03/2020 on the Processing of Data Concerning Health for the Purpose of Scientific Research in the Context of the COVID-19 Outbreak', 21 April 2020.

[170] The French regulator (the CNIL) received 14,143 complaints in 2021 and responded to a further 33,329 phone calls and 16, 898 contacts by e-mail in 2021 with advice and information (representing a 39% increase on 2020). Commission National Informatique et Libertés (CNIL), 'The CNIL in a Nutshell 2022', 4.

technologies such as smart doorbells and home security devices.[171] The diversity of contexts in which the law applies and actors within its regulatory ambit renders it impossible for regulators to provide general and authoritative guidance that is appropriate to all. Consider, for instance, the meaning of open-ended principles, such as fairness, found in the GDPR.[172] This concept could encompass both procedural and substantive fairness[173] and has been interpreted in differing ways by national regulators to date.[174] We might interpret fair processing differently if it is our neighbour processing our data compared to an international company such as Meta. Moreover, the capacity required to interpret open-ended principles such as fairness appropriately scales down badly, with individuals and small enterprises less likely to have the knowledge and resources at their disposal to do this.

In conclusion, while it is not possible to conclude authoritatively that the pursuit of complete data protection has rendered data protection ineffective, it is apparent that this completeness is in tension with effectiveness in two key ways. First, it has rendered compliance with the law's requirements practically impossible in some circumstances. As we shall see in the next section, the Court's response to such practical impossibility has been to develop an ad hoc rationalisation of the law—the responsibilities doctrine, a response which itself jeopardises the law's effectiveness. Second, the law's broad scope has further diversified the regulated community, making it more difficult for regulatees to have a shared understanding of the law and for regulators to exercise effective oversight of the broad array of data processing operations they must supervise. We will now consider how this problem might be addressed.

4. *Introducing 'Site-level' Flexibility*

Can the law be both complete and effective, as the Court aspires? The literature on the effectiveness of regulatory instruments is surprisingly

[171] Dr Mary Fairhurst v Mr Jon Wakefield (Oxford County Court) (12 October 2021), Case No: G00MK161.

[172] Article 5(1)(a) GDPR.

[173] Damian Clifford and Jef Ausloos, 'Data Protection and the Role of Fairness' (2018) 37 *Yearbook of European Law* 130.

[174] Reporting on the findings from national rapporteurs see, Orla Lynskey, 'General Report Topic 2: The New EU Data Protection Regime' in Jorrit Rijpma (ed), *The New EU Data Protection Regime: Setting Global Standards for the Right to Personal Data Protection* (Eleven International Publishing 2020) 23, 36.

sparse. Not all problems with the GDPR's enforcement stem from its broad scope. As Lancieri highlights, information asymmetries between regulators and data controllers undermine compliance and enforcement as do high levels of market power in data-related markets.[175] Some problems in Europe also stem from the difficult cooperation between regulators foreseen by the GDPR.[176] However, the problems with the law's effectiveness also stem, at least in part, from the over-inclusiveness of the law at rule level (in particular, as a result of the expanded scope of responsibility under the law). Bardach and Kagan suggest that such over-inclusiveness at rule level might be mitigated by a flexible application of the law at 'site-level'.[177] Black similarly observes the reflexive relationship between rules and enforcement: it may be possible to use over-inclusive rules knowing that their application might be tempered through a conversational model of regulation.[178]

It is possible to envisage mechanisms to facilitate such site-level accommodation in data protection law in two broad ways.[179] Such flexibility could come, firstly, through the interpretation of the law (A). Alternatively, or additionally, the law could be applied and enforced flexibly through graduated enforcement, applying insights from responsive regulation (B). These approaches are already evident to some extent in data protection law and practice yet, it is argued that without appropriate legislative underpinning and transparency regarding their application, they too risk jeopardising the attainment of the law's objectives (C).

A. *Flexible Interpretation: the Ad Hoc Rationalisation of the Law*

The undesirable effects of an over-inclusive legal framework might be mitigated by interpreting the law in a 'sensible' or proportionate manner. Moreover, calls for such a 'common sense' approach to the interpretation of data protection law have been made from inside the Court. In *Rīgas satiksme* the Court was asked to consider whether data protection

[175] Lancieri, 'Data Protection's Enforcement Gap' (n 142) 28–55.

[176] Giulia Gentile and Orla Lynskey, 'Deficient-By-Design? The Transnational Enforcement of the GDPR' (2022) 71 *International and Comparative Law Quarterly* 799.

[177] Eugene Bardach and Robert A. Kagan, *Going by the Book: The Problem of Regulatory Unreasonableness* (2nd edn, Transaction Publishers 2003) 7.

[178] Black, *Rules and Regulators* (n 132) 43–44.

[179] Practically, the remaining option for a data subject to initiate private enforcement action against a data controller for breach of the GDPR would seemingly undermine any attempt to mitigate the hard edges of the law by public enforcers applying site-level flexibility.

law provided legal grounds to compel the police to provide the personal information of an offender to a third party so that third party could initiate civil proceedings against the offender.[180] Specifically, the referring Court asked the CJEU to consider whether the legitimate interests legal basis—which enables data processing where necessary for the legitimate interests of the controller or of third parties provided such interests do not override the fundamental rights of the data subject—could be interpreted in this way. While the Court suggested this question should be answered in the affirmative, the Advocate General was more sceptical expressing a 'certain intellectual unease as to the reasonable use and function of data protection rules'.[181] In the domestic proceedings leading to the case, the police—the data controllers—had refused the request on the basis, amongst others, that alternative options to access this information were available, leading to litigation and a referral to the national regulator. For the Advocate General, the application of data protection law in this context deviated from what he saw as the main concern of the law: namely, large-scale processing of personal data by mechanical, digital means.[182] He cautioned against their application in this context suggesting that such '"application absolutism" might result in discrediting the original idea'.[183] Instead, he suggested that when balancing interests under the law, a rule of reason ought to deployed necessitating a distinction between situations entailing large-scale mechanical processing and those where a 'lighter touch' is required.[184] While this has been interpreted as a call to introduce more flexibility and less formalism into the application of proportionality assessments under the data protection framework,[185] it could also be seen as a broader appeal for more flexibility in the law's application outside the structures of

[180] Case C-13/16, *Rīgas satiksme* ECLI:EU:C:2017:336.

[181] Case C-13/16, *Rīgas satiksme* ECLI:EU:C:2017:336, Opinion of AG Bobek, para 93.

[182] ibid, para 95.

[183] ibid, para 96. As in any other area of law, rules governing certain activity must be sufficiently flexible in order to catch all the potential eventualities that arise. That might, however, lead to the danger of an overbroad interpretation and application of those rules. They might end up being applied also to a situation where the link with the original purpose is somewhat tenuous and questionable.

[184] This lighter touch would be needed in situations 'when a person is asking for an *individual* piece of information relating to a specific person in a *concretised* relationship, when there is a clear and entirely legitimate purpose resulting from the normal operation of the law'. ibid, para 98.

[185] Lorenzo Dalla Corte, 'On Proportionality in the Data Protection Jurisprudence of the CJEU' (2022) 12 *International Data Privacy Law* 259, 265.

proportionality assessments. It is noteworthy that the Advocate General refers to a rule of reason, rather than proportionality as such.

The challenges of introducing a dose of 'common sense', or site-level flexibility, to the law's application are best illustrated by the Court's designation of Google Search as a data controller and the subsequent jurisprudential contortions it has engaged in to ensure that Google's Search operations can comply with the law. In *Google Spain* the Court concluded that Google Search was a data controller and was therefore responsible for ensuring its search engine activities were compliant with data protection law. In his Opinion, the Advocate General encouraged the Court to take into consideration proportionality, the objectives of the law and the means the law contains to achieve those objectives to reach a 'balanced and reasonable outcome'.[186] His concern was that a search engine operator could not comply in law or in fact with the law's provisions leading to the 'absurd' conclusion that a search engine could not be compatible with the law.[187] This concern had also been expressed by academic observers.[188] The Court was confronted with these concerns in the later case of *GC and Others*, which laid bare the mismatch between the operations of a search engine and the law's requirements. At stake in *GC* was the prohibition on the processing of 'special category' personal data found in Article 9(1) GDPR. This provision reads as follows:

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

This provision is clearly worded as a prohibition, which is then subject to a number of exceptions found in Article 9(2) GDPR, none of which readily apply to Google's search engine activities. A literal interpretation of the law would therefore put Google's search engine operations in direct conflict with the prohibition on sensitive data processing and render them illegal. As the rules on sensitive data processing are clearly linked to the fundamental rights of individuals, the inescapable

[186] *Google Spain*, Opinion of AG Jääskinen (n 115), para 79. He deemed it inappropriate to apply a law that was drafted prior to the emergence of the decentralised internet teleologically (paras 77 and 78).

[187] ibid, paras 89 and 90.

[188] Miquel Peguera, 'The Shaky Ground of the Right to Be Delisted' (2016) 18 *Vanderbilt Journal of Entertainment and Technology Law* 507, 539.

conclusion would be that Google should cease or significantly alter its search engine operations.

In *GC*, the Court was asked to consider whether this prohibition applied to Google Search. The national referring court prefaced this question by asking whether the general prohibition also applies to search engines, 'having regard to the specific responsibilities, powers and capabilities of the operator of the search engine'.[189] The inspiration for this qualification to controller duties came from the Court in *Google Spain* when it stated that a search engine operator must ensure that its activity complies with the law's requirements 'within the framework of its responsibilities, powers and capabilities'.[190] The meaning of this phrase, and in particular its ramifications for the responsibilities of controllers under data protection law, were left unexplored until *GC and others*.

In *GC,* the Court invoked this responsibilities formula to devastating effect. It began by emphasising that the prohibition applies to all kinds of processing by all controllers[191] and that an a priori exclusion of search engines from the prohibition would run counter to its ambition of enhanced protection for such rights-infringing processing.[192] Nevertheless, the Court went on to highlight the 'specific features' of a search engine which would have an effect on the extent of its responsibility under the law.[193] In particular, as the search engine operator is responsible as a data controller by linking to existing publications, the Court held that the prohibition 'can apply to that operator only be reason of that referencing and thus via a verification, under the supervision of the competent national authorities, on the basis of a request by the data subject'.[194] The end result of *GC* is that the Court, relying on the responsibilities formula, maintained the fiction that the law applied to Google search in full, while interpreting a provision of the law clearly worded as a prohibition as a right. This ad hoc rationalisation of the law to accommodate Google's business model not only goes against a literal interpretation of the provision but also contradicts the law's general scheme.[195] The consequences of this approach will be elucidated below.

[189] C-137/17, *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* ECLI:EU:C:2019:773 para 31.
[190] *Google Spain* (n 2) para 38; repeated at para 83.
[191] *GC and Others* (n 189) paras 42 and 43.
[192] ibid, para 44.
[193] ibid, para 45.
[194] ibid, para 47.
[195] Rights of individuals are clearly found in a chapter of the law labelled 'Rights of the data subject' while the Article 9 prohibition is found in the 'Principles' chapter.

B. *Flexible Enforcement: the Role of Regulatory Discretion*

An alternative option to interpreting the law in a flexible manner would be to introduce flexibility at the point at which decisions regarding the enforcement of the law are made. Two distinct options present. Regulators might first exercise judgment in deciding which actions or complaints they will pursue. They might subsequently display further flexibility in determining how they deal with these cases.

The extent to which regulators can exercise this first-level flexibility in complaint handling under the GDPR is unclear. In other fields, the idea of risk-based regulation has taken root. This is a strategy which allows regulators to 'prioritize how they consume their limited enforcement resources such that threats that pose the greatest risks to the regulator's achievement of its institutional objectives are given the highest priority, while those that pose the least risk are allocated with few (if any) of the regulator's limited resources'.[196] European data protection regulators are already prioritising their resources in this way. The Irish regulator, for instance, states that it applies a 'risk-based regulatory approach to its work, so that its resources are always prioritised on the basis of delivering the greatest benefit to the maximum number of people'. However, while risk might be used to prioritise regulatory resources, it cannot be used as a criterion to exclude the handling of complaints entirely. The law requires regulators to 'handle complaints … and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and outcome of the investigation'.[197] Authorities have seemingly sought to stem the flow of complaints coming their way by indirectly imposing on individuals 'preliminary actions or evidence requirements that do not directly derive from the GDPR', calling into question their legality.[198] Yet, an authority cannot simply ignore a complaint or decline to deal with it as it is not a regulatory priority.[199] This is supported by the fact that data subjects have an explicit right to an effective judicial remedy against a regulator where the regulator 'does not handle a complaint or does not inform the data subject

[196] Karen Yeung and Lee A. Bygrave, 'Demystifying the Modernized European Data Protection Regime: Cross-disciplinary Insights from Legal and Regulatory Governance Scholarship' (2022) 16 *Regulation & Governance* 137, 146.

[197] Article 57(1)(f) GDPR.

[198] Access Now (n 128) 41.

[199] Hijmans, for instance, observes that 'DPAs are free to set their own agenda, but with one limitation which is their obligation to handle complaints'. Hielke Hijmans, *The European Union as Guardian of Internet Privacy* (Springer 2016), 383.

within 3 months on the progress or outcome of the complaint'.[200] Nevertheless, authorities must only handle complaints 'to the extent appropriate'. This suggests that they may inject discretion into the process at the second level of flexibility.

Flexibility in terms of the response of regulators to an infringement is in keeping with the idea of responsive regulation. Ayres and Braithwaite's influential work queried when regulators should punish and when they should persuade. Their enforcement pyramid proposed that regulators begin at the pyramid's base with persuasion moving up the pyramid to warnings and then penalties if the regulatory engagement did not have the desired effect.[201] Is such a tit-for-tat approach permitted under the GDPR? According to the Court in *Schrems II*, the primary responsibility of regulators is to monitor the application of the GDPR[202] and to ensure that it is 'fully enforced with all due diligence'.[203] Data protection regulators, which are endowed by the Charter with 'complete independence' in the discharge of their duties, might argue that such complete independence enables them to tailor the approach they take in order to ensure the 'full' enforcement of the law. This might entail starting at the bottom of the enforcement pyramid by relying on persuasion before escalating up the pyramid to credible sanctions at the top where required. Some national laws, such as the Irish Data Protection Act of 2018,[204] expressly foresee the possibility of the amicable resolution of disputes.

However, other aspects of the law appear to place a greater constraint on regulatory discretion. The provisions on administrative sanctions suggest that they were not envisaged as part of an enforcement pyramid. The GDPR text provides that regulators shall ensure that the imposition of administrative fines is effective, proportionate and dissuasive in each individual case[205] while the non-binding recitals state that penalties including administrative fines 'should be imposed for any infringement … in addition to, or instead of appropriate measures imposed by the supervisory authority'.[206] By way of exception, it specifies that for minor

[200] Article 78(2) GDPR.
[201] Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 2002) 35.
[202] Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II)* ECLI:EU:C:2020:559, para 108.
[203] ibid, para 112.
[204] S.109(2) Data Protection Act 2018 (Ireland).
[205] Article 83(1) GDPR.
[206] Recital 148.

infringements or if the fine would constitute a disproportionate burden to a natural person, a reprimand may be issued instead of a fine. Erdos, for instance, claims that the GDPR therefore establishes a presumption that a national data protection authority will 'at least take formal corrective action once cognisant of a significant infringement of data protection law'.[207] This seems also to be borne out by the wider text of the GDPR. The idea of amicable dispute resolution is mentioned only once in a recital and, only then, in the context of disputes that are localised because of their nature or impact.[208] We could conclude that, at a minimum, amicable resolution is inappropriate in the context of transnational disputes which might require cooperation between various concerned authorities. It is notable also that while data subjects have the right to challenge a regulator before a Court where it does not handle a complaint or where it issues a legally binding decision[209] this seems to leave a gap in situations where the complaint is handled but no legally binding decision is adopted.[210] Again, this suggests that the legislature did not foresee such flexible enforcement of the rules at scale. Beyond the doctrinal question of whether data protection law allows for the exercise of such site-level discretion, this discretion also raises broader normative challenges to which we shall now turn.

C. *The Challenges of Site-Level Flexibility*

In an ideal world, the 'unreasonable and excessive legal consequences'[211] of the broad scope of application of data protection law might be avoided or mitigated by interpreting and enforcing the law flexibly while continuing to offer effective and complete protection to individuals. The reality, however, is that site-level flexibility itself entails potential negative repercussions that must be addressed. Two negative consequences stand out: these concern the effectiveness and the quality of the law, respectively.

[207] David Erdos, 'Ensuring Legal Accountability of the UK Data Protection Authority: From Cause for Data Subject Complaint to a Model for Europe?' (2020) 5 *European Data Protection Law Review* 444, 452.

[208] Recital 131.

[209] Article 78(2) and (1), respectively.

[210] A lacuna explored, but not filled, in the UK case of *Killock & Veale v ICO* [2021] UKUT 299 (AAC).

[211] *Google Spain*, Opinion of AG Jääskinen (n 115) para 30. He highlighted that currently 'the broad definitions of personal data, processing of personal data and controller are likely to cover an unprecedentedly wide range of new factual situations due to technological developments'.

(i) *The effectiveness of the law*

The impact that the flexible interpretation and enforcement of data protection law will have on the law's effectiveness remains uncertain. In *GC* the Court was left with a choice: to declare Google Search's data processing, and therefore its business model, to be incompatible with the law or to accommodate the business model. The Court's solution—treating an ex ante prohibition as an ex post right—does the latter: it is a bespoke interpretation of the law designed to accommodate a business model that does not fit the mould. It has been suggested that this finding provides a 'safety valve' against the disproportionate extension of data protection obligations to search engine operators.[212] Such accommodation might be justified on the basis of the societally beneficial role search engines play in organising the world's information.[213] It was likely for this reason that the Advocate General considered that any finding of incompatibility with the law by search engines would be absurd. Yet, the relationship between law and technology in this instance is worth highlighting. The law is often simplistically characterised as seeking to keep up with technology, however, in *GC* we see that technological design impacts the interpretation and application of the law.[214] Specifically, the responsibilities formula deployed by the Court to rationalise the law's application means that technologies that are designed in a way that renders data protection compliance impossible may avoid the law. It is thus no longer safe to assume that when there is personal data processing, 'the entire body of the data protection guarantees applies'.[215] The Court's approach is likely to embolden proponents of the 'move fast and break things' model of technological practices and design. We might, for instance, query whether data protection rights such as the right to delete can be exercised on an immutable decentralised ledger technology such as blockchain[216] or whether a tool like ChatGPT could avoid ex ante or ex post data protection requirements as they are not commensurate with the 'powers, capabilities and responsibilities' of the relevant data controllers. In short, the risk is that the responsibilities formula creates an incentive for technologists to circumvent the law through

[212] De Gregorio (n 114) 141.

[213] For a more critical assessment of the power wielded by Google Search see Powles (n 117).

[214] Therefore while it is often claimed that the law is designed to be technologically neutral, we cannot claim that the law applies in a way that is technologically neutral.

[215] Purtova, 'The Law of Everything' (n 9) 71.

[216] Michèle Finck, 'Blockchains and Data Protection in the EU' (2018) 1 *European Data Protection Law Review* 17, 30–31.

design, a scenario that almost certainly militates against effective data protection.[217]

Nor is it clear that the flexible enforcement of the law will yield more effective data protection. While it is generally acknowledged that the success of data protection law should not be measured using a crude assessment such as the number of fines issued,[218] this is in part because the law offers a broader array of corrective powers that regulators can draw on, such as a ban on data processing operations, that may have an equally, if not more significant effect, than fines.[219] Evidence to date indicates that European data protection regulators have made limited use of the full palette of corrective powers.[220] If flexible enforcement, anchored in the enforcement pyramid, secured the more effective application of data protection law, a purposive interpretation of the law would support its application. However, we lack the empirical evidence needed to assess whether flexible enforcement leads to more effective protection. In situations where the overall level of formal enforcement drops dramatically due to a regulatory preference for informal interactions between regulators and regulatees, doubts arise as to the impact of the law in practice. For instance, in the UK although the regulator 'handled' 40,000 data subject complaints in the 2021–2022 period only four fines were issued for breach of the GDPR totalling £663,000 in total.[221] No other enforcement notices or penalties were issued. Some of the examples of situations where the regulator opted not to use its formal enforcement powers are striking. For instance, the Information Commissioner's Office (ICO) did not impose an administrative sanction on two police forces that surreptitiously recorded and stored over 200,000 phone conversations involving victims, witnesses and perpetrators of suspected crimes as part of its revised approach towards the public sector.[222] We might legitimately query in these circumstances

[217] System design cannot only frustrate rights but often entails trade-offs between rights that are not made explicit by the law. See further, Michael Veale, Reuben Binns and Jef Ausloos, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8 *International Data Privacy Law* 105.

[218] Commission Staff Working Document (n 127) 5.

[219] European Parliament, 'European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP))' [2021] C494/29, para 13.

[220] EDPB, 'Overview on resources' (n 134) 14.

[221] ICO, Information Commissioner's Annual Report and Financial Statements 2021–22 July 2022 HC 392, 33.

[222] ICO, 'ICO reprimands Surrey Police and Sussex Police for recording more than 200,000 phone calls without people's knowledge', 18 April 2023.

whether informal enforcement is delivering effective fundamental rights protection.

(ii) *The quality of the law*

The flexible interpretation and application of the law is difficult to square with some of the core qualities of law that ensure its internal morality, including that law be general, publicly promulgated and that there be congruence between official action and declared rule.[223] This is particularly important in the data protection context where the foreseeability of the law is a requirement to justify interferences with fundamental rights[224] while the foreseeability of data processing operations is central to garnering public trust in processing and technology.[225]

The data protection framework is 'all or nothing' in so far as it applies when the data processed is personal but not to non-personal data.[226] However, it has arguably never been accurate to characterise the data protection framework as a one-size-fits-all model, or an 'intensive and non-scalable regime of rights and obligations'[227] due to the existence of the general principle of proportionality and the introduction of risk-management obligations. These already introduce a significant degree of flexibility into how the law is interpreted. For instance, Gellert observes that while the GDPR provides some guidance to data controllers regarding potential sources of risk (toxicological factors) it leaves the consequences and harms (epidemiological factors) as well as the methodologies for assessing harms undelineated to a large extent.[228] However, the use of the responsibilities formula marks a qualitative shift in the

[223] Fuller (n 146). These criteria also reflect those set out by Diver in his work on the optimal precision of legal rules. He notes that the success of a rule will depend on qualities such as its transparency (whether the words have a well defined and universally accepted meaning within the relevant community) and their accessibility (their application to concrete situations without excessive difficulty or effort). Colin S. Diver, 'The Optimal Precision of Administrative Rules' (1983) 93 *Yale Law Journal* 65.

[224] Joris van Hoboken, 'From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and US Frameworks for Personal Data Processing' in Bart van der Sloot, Dennis Broeders and Erik Schrijvers (eds), *Exploring the Boundaries of Big Data* (Amsterdam University Press 2016) 231, 248.

[225] Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic, and Limits* (Kluwer Law International 2002), 107–112.

[226] Koops (n 9) 257.

[227] Peter Blume, The Data Subject, (2015) 1 Eur Data Prot L Rev 42.

[228] Gellert (n 11) 215.

law's flexibility.[229] While some may welcome a doctrine that enables the application of the law to be calibrated to the powers of the data controller,[230] this must be set against the uncertainty that this formula introduces about how the rules apply to whom. Unlike other elements of the legal regime which also introduce elements of scalability, such as the provisions introducing risk-management requirements, the application of this formula comes with no guidance or legislative footing. Quelle suggests that this gap could be filled by applying the responsibilities formula with reference to risk.[231] While this may help to anchor the application of the responsibilities formula more firmly to the text of the GDPR in some circumstances, it would not be helpful when interpreting provisions where there is no reference made to risk. The result will be the further unpredictability of the regime's application to the detriment of not only its effectiveness but also its transparency and predictability.

Moreover, while the 'rule of reason' applied by the Court might be likened to the principle of proportionality, proportionality analysis does not feature explicitly at all in the Court's reasoning. Like the application of the rule of reason in competition law, where a restriction on competition was removed from the scope of competition law as this restriction was inherent in the pursuit of public policy objectives, this might be characterised as 'bold and innovative or unprincipled and misconceived'[232] depending on one's perspective. More generally, the extent of the role that proportionality could play in introducing flexibility to the law's application remains ambiguous. If the data protection framework is correctly characterised as a justificatory framework for data processing that interferes with fundamental rights, then the provisions of the GDPR and their interpretation should embody the principle of proportionality. Primarily through the jurisprudence of the Court, proportionality has emerged as a 'data privacy principle in its own right' with

[229] The role of risk in data protection law remains ambiguous. As Yeung and Bygrave note, although regulatory scholars are familiar with the idea of 'risk' in various guises, the concept of 'risk to rights' is unfamiliar and the traditional focus of risk on quantifying tangible harms sits uneasily alongside the dignitarian basis for human rights. Yeung and Bygrave (n 170) 143.

[230] Quelle, for instance, suggest that this formula serves the function of maintaining a broad scope of application for the data protection rules while 'keeping the consequences of controllership in check'. Claudia Quelle, 'GC and Others v CNIL on the Responsibility of Search Engine Operators for Referring to Sensitive Data: The End of 'Right to be Forgotten' Balancing?' (2019) 5 Eur Data Prot L Rev 438, 440.

[231] ibid.

[232] Giorgio Monti, 'Article 81 EC and Public Policy' 2002(39) *Common Market Law Review* 1057, 1088.

some viewing it as being 'at the core of the GDPR's structure'.[233] While the data protection principles do not explicitly include proportionality, it is said to underpin them and 'shines through in their interstices'.[234] Proportionality therefore potentially offers a more rigorous tool through which to introduce flexibility into the data protection framework. This, however, depends on how the proportionality principle is applied. The Court has, for instance, on occasion replaced an assessment of whether data processing was compatible with the specific provisions of the GDPR with a more general assessment of whether the processing was compatible with the principle of proportionality, grounding its reasoning directly in the EU Charter rights to data protection and to respect for private life.[235] Regulators are more likely than Courts to engage in a more loyal and specific application of the law's provisions than to replace their application with a broader proportionality analysis, as the Court did in this case. Moreover, while some provisions of the law lend themselves readily to proportionality analysis,[236] notably the principles found in Article 5 GDPR, many of the law's other ex ante requirements, such as transparency obligations and the abovementioned prohibition on special category data processing, are less amenable to proportionate interpretation. The appropriate role of this principle in calibrating the application of data protection law, and its relationship with the risk requirements introduced by the GDPR, requires further research and consideration.

The compatibility of responsive regulatory enforcement with rule of law requirements has received surprisingly little attention.[237] The complete independence of data protection authorities dictates that these regulators exercise their powers free from internal and external influence. However, some accountability mechanisms must exist if

[233] Lee A. Bygrave, *Data Privacy Law: an International Perspective* (OUP 2014) 147; De Gregorio (n 114) 141.

[234] Lee A Bygrave and Dag Wiese Schartum, 'Consent, Proportionality and Collective Power' in Serge Gutwirth and others (eds), *Reinventing Data Protection* (Springer 2009), 162.

[235] Case C-439/19, *Latvijas Republikas Saeima (Points de pénalité)* EU:C:2021:504, para 97.

[236] ibid, para 98. In the penalty points case, the Court affirmed that the principle of data minimisation (Article 5(1)(c) GDPR) 'gives expression to the principle of proportionality'.

[237] Jan Freigang, 'Is Responsive Regulation Compatible with the Rule of Law' (2002) 8 *European Public Law* 463.

regulators fail to discharge their primary responsibility of enforcing the law.[238] The status quo also does nothing to prevent zealous application of the law, such as fining individuals for the positioning of their home or business surveillance cameras or for posting content filming public disorder incidents on social media.[239] The transparency of the criteria applied in deploying the enforcement pyramid will be critical in this regard.[240] For instance, the ICO has adopted a revised approach towards the public sector, where it has opted to use its discretion to reduce the impact of fines on public sector operators. Pursuant to this approach, the ICO will rely on powers to warn, reprimand and issue enforcement notices, with fines only handed down in the 'most serious cases'.[241] However, the example mentioned above of the covert recording of conversations by the police where no fine was issued begs the question of what the ICO considers to be a 'serious case'. More broadly, empirical evidence suggests that where regulators have adopted a strategic approach to enforcement this has neither been calibrated to the extent to which the data controllers demonstrated compliance with relevant legal requirements nor systematically assessed against the overarching requirement to achieve effective and complete protection of data subjects.[242]

In the absence of clear and transparent criteria guiding the enforcement of the law, the ensuing regulatory roulette offends against the equal protection and application of the law to the detriment of its beneficiaries—individuals in the first instance but ultimately society. Moreover, it may be inappropriate to apply the 'conversational approach' to the enforcement of the law, found at the bottom of the enforcement pyramid, in some circumstances. These includes where the stakes are high (such as in situations where there is a risk of irreversible harm); where

[238] Erdos, 'Ensuring Legal Accountability' (n 207). The one-stop-shop and consistency mechanisms foreseen in Chapter VII, Sections 1 and 2 GDPR are ill equipped to force an authority to handle a complaint in a particular manner: Gentile and Lynskey (n 176).

[239] Easy GDPR, 'GDPR fine for Austrian kebab store', https://easygdpr.eu/en/gdpr-incident/gdpr-fine-for-austrian-kebab-store/; One Trust Data Guidance, 'Spain: AEPD fines individual €6,000 for unlawfully processing personal data' https://www.dataguidance.com/news/spain-aepd-fines-individual-600-data-minimisation

[240] The importance of transparency in this regard has been emphasised by the European Parliament which has called for harmonisation of penalties by means of guidelines and clear criteria 'in order to increase legal certainty and to prevent companies settling in the locations that impose the lowest penalties'. European Parliament (n 191) para 13.

[241] ICO, 'ICO Sets Out Revised Approach to Public Sector Enforcement' (30 June 2022).

[242] Erdos *Balancing on a Tightrope* (n 14) 199.

there are no repeated interactions with regulatees; or where the regulatee is reluctant to comply.[243]

5. *Conclusion*

Data protection law faces mounting criticism, both from human rights scholars and activists and from those who treat it as an unnecessary impediment to boundless data processing and the claimed innovation this would entail. Despite the technological developments during its lifespan, it has proven to be a resilient and adaptable legal framework, most recently acting as a first brake on the deployment of generative AI in ways that violate fundamental rights. The expansive interpretation of responsibility under the law has already yielded some benefits. Equally, however, many of the challenges that the law faces stem from its application, not to everything, but to everyone. While we could think of data protection as a broad church, it has also been characterised (perhaps more accurately) as an indiscriminate obsession.[244] Thinking about the law's future, we could be pulled in different directions. On the one hand, it is challenging to interpret the law in way that adheres to different contexts while, on the other, its broad application puts regulators under pressure with rising numbers of complaints which they have an imperative to handle. The judicial response has been to overlook these problems, or to simply patch them by rationalising the law's application in an ad hoc manner.

Turning to the future, the possibility of using increased site-level flexibility must be further explored and the rule of law challenges it entails addressed. This can be done by the EDPB without legislative change under the auspices of the GDPR. More broadly, however, it is clear that the current lack of empirical assessment of how the law applies in practice 'leaves legal reformers shooting in the dark, without a real understanding of the ways in which previous regulatory attempts have either promoted or thwarted privacy's protection'.[245] Recognising that no law is ever fully enforced, what is required for data protection is agreement on an appropriate standard against which to gauge regulatory

[243] Black, *Rules and Regulators* (n 132) 43–44.

[244] Roger Brownsword and Morag Goodwin, *Law and the Technologies of the Twenty-First Century: Text and Materials (Law in Context)* (CUP 2012), 310.

[245] Kenneth A. Bamberger and Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (MIT Press 2015), 9.

effectiveness. Determining an appropriate balance between data protection compliance and data protection enforcement will be necessary. Finally, and perhaps most ambitiously, the purposes of data protection law need to be further specified by the Court. A starting point may be to disentangle the intersecting demands of informational privacy from those of fair information governance.[246]

This may seem like an uphill battle. Data protection pioneer, Spiros Simits, spoke of data protection as an 'impossible task'.[247] However, Simitis also saw data protection as an 'unending learning process' necessitating a 'continuous critical review of the regulatory approach' to ensure its efficiency.[248] It is in this spirit that the challenge of securing effective fundamental rights protection in the digital era should be approached.

[246] Brownsword and Goodwin (n 241) 312.
[247] Simitis (n 119).
[248] ibid.