Demystifying the modernized European data protection regime

Yeung, Karen; Lee A, Bygrave

DOI:
10.1111/rego.12401

Document Version
Publisher's PDF, also known as Version of record

Citation for published version (Harvard):
Yeung, K & Lee A, B 2021, 'Demystifying the modernized European data protection regime: cross-disciplinary insights from legal and regulatory governance scholarship', *Regulation & Governance*.
https://doi.org/10.1111/rego.12401

Regulation & Governance

Regulation & Governance (2021) doi:10.1111/rego.12401

Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship

Karen Yeung

Birmingham Law School & School of Computer Science, The University of Birmingham, Birmingham, UK

Lee A. Bygrave

Norwegian Research Center for Computers and Law, Department of Private Law, University of Oslo, Oslo, Norway

Abstract

This article critically examines fundamental aspects of the recently reformed European regime for protection of personal data, focusing on the General Data Protection Regulation (GDPR) adopted by the European Union (EU) in 2016. Although the GDPR is now a central concern for many organizations across multiple sectors, many complain that it is arcane, confusing, and complex. By combining knowledge from two disciplinary perspectives – from regulatory governance scholarship, on the one hand, with legal scholarship from the fields of data protection law, constitutional law, and fundamental rights, on the other hand – this article seeks to "demystify" the key elements of the regime's architecture and approach in light of the significant uncertainties concerning the nature of its requirements. In particular, this article examines the tension between the regime's pronounced "risk-based" approach to compliance and its basic objective of safeguarding fundamental rights, and the challenges facing data protection authorities in providing timely clarifications of the regime's norms. We argue that, despite its complex and arcane character and continuing uncertainty about the precise scope of its requirements, the regime is an innovative hybrid with a significant degree of in-built "future-proofing" that should help render it more resistant to being rapidly overtaken or outpaced by organizational–technological developments. The secondary aim of this article is to demonstrate how academic insights from two distinct but related disciplinary perspectives – legal scholarship and regulatory governance studies – offer a potentially fruitful approach to enrich understandings of the European data protection regime in particular, and of the mechanics, efficacy, and legitimacy of regulatory governance regimes more generally.

Keywords: data protection, data protection authorities, fundamental rights, regulatory governance, risk management.

1. Introduction

Data protection law appears to be thriving in Europe. The adoption of the General Data Protection Regulation (GDPR)[1] in 2016 has reinvigorated the European regulatory framework for the processing of personal data. European data protection law is now a central concern for numerous organizations and individuals who previously ignored it or regarded it as having marginal significance. As policy-makers everywhere struggle to assess whether new regulatory measures are needed to address the threats posed by the "rise of the machines" (especially "smart" machines), many believe data protection legislation will play a key role in securing "algorithmic accountability" in the coming years (see e.g. European Commission 2020a, pp. 16, 19). Yet many also claim that Europe's reinvigorated data protection regime suffers from both complexity and uncertainty about the scope, content, and contours of its demands and how those uncertainties will be resolved.[2] Hence, many of its substantive provisions, along with the mechanisms upon which it relies, remain puzzling, even for data protection law specialists. The primary aim of this article is to examine specific dimensions of the GDPR that have been regarded as unclear, if not bewildering, and thus subject to criticism. In seeking to "demystify" key aspects of its

Correspondence: Karen Yeung, Birmingham Law School & School of Computer Science, The University of Birmingham, Birmingham, UK. Email: k.yeung@bham.ac.uk

Conflict of interest: The authors declare no conflicts of interest.

Accepted for publication 29 March 2021.

architecture and approach, we draw upon and integrate selective insights from two disciplinary perspectives: those from regulatory governance scholarship (particularly literature concerned with the tools and techniques of government including so-called "risk-based" regulatory approaches) on the one hand and insights from scholars of data protection law, constitutional law, and fundamental rights on the other. Notwithstanding long-running contestation about the overarching objectives of European data protection law, the GDPR can be understood as a regulatory governance regime in that it is fundamentally *purposive* in nature, entailing an organized attempt to achieve some prespecified objective or objectives involving behavioral change or the management of risk (Lodge & Wegrich 2012; Black 2014; Gellert 2020). In this respect, the GDPR establishes a regime that regulates the collection and further processing of personal data in Europe in order to safeguard fundamental rights while promoting a flourishing European data economy. The secondary aim of this article is to demonstrate how our methodological approach, which draws upon two distinct yet complementary disciplinary perspectives, can offer an enriched understanding of the GDPR and may offer a lens through which the effectiveness and legitimacy of regulatory governance regimes more generally might be examined. This is particularly important in relation to ongoing policy and academic debates concerned with the regulation of Artificial Intelligence (AI), which often fail to refer to, or demonstrate awareness of, the rich body of scholarship we refer to as "regulatory governance" studies. Admittedly, the precise content and contours of this body of work as a distinct field of scholarly inquiry are broad, unsettled, constantly shifting, and variously understood (Baldwin *et al.* 2010) partly because it draws from a wide range of disciplines and perspectives within the humanities and the social sciences. Yet what unites these otherwise disparate strands of literature is a shared focus on the purposive shaping of social behavior entailing the tripartite functions that are present in any cybernetic control system, namely those of standard-setting, information-gathering, and behavioural modification (Hood *et al.* 2001).

The immense variety of regulatory governance scholarship offers a broader panoply of analytical taxonomies than our analysis can meaningfully draw upon, given space constraints. Thus, our analysis necessarily draws selectively (and rather briefly) on concepts utilized by regulatory governance scholars that we consider particularly helpful in illuminating the contemporary concerns and criticisms about the European data protection regime. Many of these criticisms coalesce around complaints about the regime's complexity and a persistent lack of clarity in relation to the multiple mechanisms and concepts through which its provisions are operationalized, particularly those that are relatively untested as regulatory tools. Accordingly, our discussion focuses on three distinct yet interlinked dimensions of the regime that have attracted criticism. It begins with an examination of the design, structure and techniques upon which the regime relies, drawing on elements of a well-established strand of literature concerned with regulatory instruments and techniques (or "tools of government" in the parlance of public administration). Secondly, it considers the role of fundamental rights within the regime as a foundational objective and the relationship between rights and risk in light of continuing uncertainty about what a "risk-based" approach to compliance associated with the regime's modernization requires. Here, we build upon a small but growing body of data protection law scholarship concerned with the role of risk within the GDPR, seeking to elucidate the concept of a "risk to rights" upon which it relies, with the aim of demonstrating how it can be illuminated by, and distinguished from, regulatory governance research and practice concerned with risk, risk assessment, and "risk-based regulation," yet in a way that is sensitive to the jurisprudential character and structure of fundamental rights. Thirdly, this article considers the regime's institutional dimensions in light of criticisms that significant uncertainty persists concerning what, precisely, it requires of regulated organizations. Here, we focus on the critical role of national data protection authorities ("DPAs") in giving flesh to the regime, including challenges associated in meeting competing demands placed on them. To this end, we draw on regulatory scholarship highlighting the dilemmas faced by nonelected, independent regulatory agencies in seeking to secure and maintain their legitimacy within democratic societies. The final section concludes.

2. Institutional mechanisms and regulatory techniques

The European data protection regime's structural and technical complexity renders it largely incomprehensible to non-specialists. Small- and medium-sized enterprises (SMEs) report significant difficulties in understanding the GDPR's requirements, forcing them to seek costly advice from external specialists (Multistakeholder Expert Group 2019, p. 4). This complexity is partly due to its reliance on multiple regulatory techniques, some of which

are relatively novel and untested. The following discussion steps back from the detail of the regime's legislative provisions by drawing on insights and concepts concerned with the "tools of government," some of which may be rather abstract and unfamiliar to data protection lawyers, to bring into sharper focus the underlying mechanisms through which the GDPR is intended to work. For this purpose, it is important to acknowledge that academics have sought to classify and understand regulatory instruments in many different ways, none of which can claim pre-eminence (Morgan & Yeung 2007, p. 79). Thus, for example, in the realm of internet governance Lessig's fourfold taxonomy of modalities of control that distinguishes between law, markets, social norms, and code (Lessig 1999) and which can be understood as a variant of the tripartite typology of social coordination mechanisms consisting of hierarchy, markets, and networks (Thompson *et al.* 1991) is a popular starting point for analysis. This contrasts with the distinction between "carrots, sticks, and sermons" (Bemelmans-Videc *et al.* 1998) beloved of many public administration scholars. Likewise, the rich scholarly literature concerned with the nature, scope, and formulation of rules and standards offers a large range of vantage points, which do not always receive mutual recognition. So, for example, Anthony Ogus's seminal work, *Regulation – Legal Form and Economic Theory*, devotes considerable attention to the role of criminal law in support of standards (Ogus 2004), whereas the *Oxford Handbook of Regulation* makes no reference to the criminal law in its subject index, and nor does criminal liability form the focus of any of the individual chapters (Baldwin *et al.* 2010). Because our aim is to offer an explanatory account of the distinctive architectural features of the European data protection regime, the following discussion draws selectively in Section 2.1 on this literature, examining the character of the core data protection principles underpinning the GDPR by reference to the claimed distinction between rules vs. principles, on the one hand, and performance- vs. outcome-based standards on the other. In Section 2.2, it examines the role of command, design, and "meta-regulation" as key "modalities of control" through which the regime's architecture can be helpfully understood.

2.1. Understanding the principles of fair information practice

A central anchoring point for many of the regime's substantive norms is the core data-processing principles laid down in Article 5 GDPR and which are reflected in other provisions of the Regulation, such as Article 6. These principles provide, inter alia, that processing of personal data shall occur lawfully, fairly', and in a transparent manner (principle of "lawfulness, fairness, and transparency"), for specified legitimate purposes and not for subsequent incompatible purposes (principle of "purpose limitation"), that the data shall be adequate, relevant, and limited to what is necessary in relation to the purpose for which they are processed (principle of "data minimization"), and that the data shall be subject to appropriate security measures (principle of "integrity and confidentiality"). The principles largely replicate the "fair information practice principles" (FIPPs) originating from the mainframe computing era of the early 1970s. When the GDPR was drafted, most European law-makers believed that the FIPPs had stood the test of time, needing only relatively minor tweaking and reinforcement, such as the addition of a principle of "accountability" laid out in Article 5(2) GDPR ("The controller[3] shall be responsible for and be able to demonstrate compliance with, paragraph 1 ('accountability')").

Two strands of regulatory governance scholarship concerned with the challenges and trade-offs associated with standard-setting can deepen our understanding of how these principles are intended to operate: literature concerned with the relative strengths, shortcomings, and experience of (i) "performance-" or "outcome-based" standards relative to "process-based" standards (see e.g. Black *et al.* 2007; Lodge & Wegrich 2012, p. 15), and (ii) detailed rules relative to broadly framed "principles" (see e.g. Diver 1983; Braithwaite 2001). Outcome- or performance-based standards have typically been preferred to process-based standards because they offer greater flexibility and freedom to regulated parties in determining how to meet a specified policy objective. This avoids the one-size-fits-all approach typically characterizing standards that mandate compliance with a set of specified processes. Outcome-based standards are also believed to be more amenable to measurable performance (such as air quality) and less prone to circumvention or avoidance. However, recent regulatory failures have vividly illustrated how outcome-based approaches can be gamed and are vulnerable to the problem of "teaching to the test" (Coglianese 2017), as the recent VW "Dieselgate" scandal exemplifies. They may also require significant levels of professional knowledge to evaluate whether key substantive requirements have been met, and this knowledge may be in short supply.[4] These sorts of

challenges could arise, for instance, in evaluating compliance with the GDPR's information security requirements (Article 32 GDPR), which are a form of relatively concrete outcome-based standards that rely on technical expertise for their elucidation. However, the regulatory agencies involved, including DPAs, CERTs (Computer Emergency Response Teams), and ENISA (the EU Cybersecurity Agency), tend to have significant in-house expertise much of which they share among themselves, thereby reducing the risk of undue deference to professionals employed by industry.

Moreover, the FIPPs that help form the core of EU data protection norms are neither *clearly* outcome-based nor process-based in character. Rather, they are a hybrid: they restrict the *processes* by which personal data must be handled, yet do so in ways that require conformity with particular *substantive values or outcomes*, such as requirements of accuracy, lawfulness, security, and the like. The underlying rationale for this approach might be an attempt to combine the "best of both worlds": on the one hand, the procedural focus arguably reflects uncertainty on the part of legislators about the nature of the interests at stake, along with a desire to maintain regulatory flexibility in the face of technological complexity and change (Burkert 1988, pp. 384–85), while the explicit reference to norms that require judgments about compliance with substantive values, such as lawfulness and legitimacy, suggests that unthinking adherence to a set of routine procedural checklists will not suffice.

The formulation of the regime's core principles in broad, rather sweeping terms, can also be explained by reference to legal and related scholarship concerned with understanding the dilemmas which arise in drafting appropriate norms and standards. A contrast is often drawn between tightly specified, detailed rules on the one hand, and broadly drafted "principles" on the other (Ford 2010). Diver (1983) argued that a rule's success in fulfilling its purpose depends largely on several qualities: its transparency (does the wording of the rule have a well-defined and universally accepted meaning within the relevant community?), its accessibility (is the rule applicable to concrete situations without excessive difficulty or effort?), and its congruence with the underlying policy objective (does the substantive content of the message communicated by the rule's wording produce the desired behaviour?). Trade-offs between these qualities are unavoidable so that, for example, detailed, narrowly specified rules may be highly transparent and accessible but fail to achieve the desired behavioural outcome and are prone to problems of "gaming" and "creative compliance" through formalist rule interpretations in ways that contravene their underlying "spirit" (McBarnet & Whelan 1991). Although broadly drafted principles may be highly congruent with the rule-maker's underlying policy objective, they often suffer from a lack of transparency and accessibility (Diver 1983).

The broad-brush formulation of the GDPR's data protection principles offers little up-front guidance concerning how, precisely, they are to be understood and implemented. This is true of many of the GDPR's other provisions. Yet drafting legal rules in broad terms does not necessarily generate uncertainty for their addressees, particularly if there are widely shared understandings of key terms within the relevant "interpretative community" (Black 2008). Such understandings are more likely to arise within sector-specific regulatory regimes where the regulated sector forms a relatively tight-knit community (e.g. the nuclear power industry). However, a distinctive and important feature of the GDPR is its universality: it applies to *all* those who collect and process personal data (apart from situations of processing in the course of a purely personal or household activity: Article 2(2)(c) GDPR), and thus to individuals and organizations, whether public or private, of all shapes and sizes. Most regulatees will therefore need to seek expert legal advice concerning the application of the GDPR's rules, increasing their costs. For start-ups and SMEs, these costs will be more difficult to absorb than for the digital Goliaths with a "move-forward-and-break-things" business mentality supported by massive litigation budgets. As for data subjects, this interpretative ambiguity might be double-edged. Although they undoubtedly welcome both the enhancement of their rights and the boost to DPAs' powers of enforcement under the reformed legislative provisions, the interpretative flexibility of the regime's principles could make the assertion of their rights more difficult in practice, particularly against the digital Goliaths. This, in turn, could operate in practice to support the interests of the powerful rather than providing workable tools of empowerment for data subjects. Accordingly, the institutional structure, experience, and enforcement activities of the organizations tasked with responding to this interpretative uncertainty will play a vital role in how the regime operates in practice – a matter discussed more fully in Section 4.

2.2. Regulatory architecture, tools, techniques, and mechanisms of constraint

Characterizing the structure of the GDPR's data protection principles tells us little about how they are intended be operationalized. Accordingly, the following section critically examines many of the key techniques, instruments and regulatory modalities through which the regime is intended to take effect by drawing selectively on a well-established literature on regulatory tools and techniques that straddles regulatory governance studies and public administration. We focus on three categories of technique: "command-and-control," meta-regulation, and "design-based" regulation. We do so because they each describe essential elements of the regime, even if – as we demonstrate – none of these on their own adequately captures its essence. Furthermore, the categories of meta-regulation and design-based regulation have received relatively little attention in legal scholarship on data protection (largely because these techniques have not figured prominently in previous generations of data protection laws), and design-based regulation has received relatively little attention in regulatory governance scholarship apart from the literature concerning governance of the internet. Both categories are, however, key features of the revamped EU regime.

2.2.1. Command and control

The GDPR's basic structure and premise manifests a conventional "command-and-control" strategy, comprising a set of legislative norms (or "commands") which must be complied with by those who wish to process personal data (i.e. data controllers and processors) (Gellert 2020). Failure to comply (or to find a proper derogation from the norms) renders the resulting data-processing activities unlawful and exposes data controllers and processors to enforcement action initiated by DPAs or data subjects, potentially attracting significant penalties. The GDPR radically beefs up this sanctions regime.[5] This has provoked considerable angst for data controllers and processors while accentuating the regime's command-and-control profile. The introduction of a raft of new requirements concerning, for instance, the processing of children's data (Article 8), data protection by design and by default (Article 25), data breach notification (Articles 33–34), and impact assessment (Article 35) reinforces this profile.

2.2.2. Design-based regulation: Data protection by design and by default

Among the most innovative of the GDPR's new requirements are those concerned with "data protection by design and by default" which, in essence, impose legal obligations on data controllers (and, indirectly, data processors) to "hard wire" data protection norms into information systems development (Article 25 combined with Articles 28(1) and 24), thus mandating the use of "design-based" regulatory techniques (Yeung 2008; Hildebrandt 2011; Yeung 2015; Bygrave 2017a). These obligations pertain to the design of software, hardware, and the data controller's business strategies and other organizational practices. They reflect a conviction that building data protection principles into information systems architecture will substantially improve their traction reflecting the regime's aims of both "minding the machine" and actively seeking to "mould" it (Bygrave 2019, p. 247). Accordingly, the GDPR transcends the "code versus law" discourse that often portrays "West Coast code" (software programs and the like) and "East Coast code" (legislation) as competing modalities of control (Lessig 1999; Lessig 2006), and evinces a belief that technology can be applied in the service of interests that it concurrently threatens, if required by law. The vision underlying Article 25 seeks to embed the values of EU data protection law into information systems architecture such that the resultant "lex informatica" (Reidenberg 1997) will render the GDPR largely self-enforcing. For example, Bayamlıoğlu argues that, properly understood, Article 25 requires that machine learning models used to process personal data are designed and configured to produce computational models that are more amenable to human interpretation, provided this is technically and economically feasible (Bayamlıoğlu 2021). Although the provisions of Article 25 are formulated in relatively open-ended terms, with extremely broad qualifications that leave controllers with considerable discretion, DPAs have already issued fines for their violation (Bygrave 2020, p. 579).

2.2.3. Meta-regulation and data protection impact assessments

Despite the regime's command-and-control framework, it also relies heavily on the active participation of regulated organizations in standard setting and managing the risks associated with processing personal data, albeit directly underpinned by the law's authoritative backing. Accordingly, the regime can be understood as utilizing strategies of "meta-regulation," pursuant to which "regulators do not prescribe how regulatees should comply,

but require them to develop their own systems for compliance and to demonstrate that compliance to the regulator" (Black 2012, p. 1045; Black 2005). The alleged benefits of meta-regulation lie in enabling the regulated organizations to design systems and processes that are better suited to ensuring compliance within their own organization, and placing the onus on them to demonstrate compliance (rather than placing the onus on regulators to demonstrate non-compliance). It can also foster improved regulatory outcomes and enhanced legitimacy via market or "community"-based governance (Black 2012, pp. 1045–1048). Elements of meta-regulation are evident in the GDPR's design, in so far as they entail some kind of "outsourcing" of regulatory responsibility to regulated organizations, subject to oversight by the regulator, such as provisions permitting industry associations and the like to devise "codes of conduct" (Articles 40–41).[6] However, while these provisions are more extensive than under the GDPR's predecessor, the 1995 EU Data Protection Directive, the precise legal status of approved codes remains uncertain, particularly the extent to which they may operationally replace legislative provisions dealing with the same subject matter such that their breach constitutes a breach of the law.

One of the GDPR's most significant forms of meta-regulation concerns the legal duty imposed on data controllers to undertake a data protection impact assessment (DPIA) prior to the processing of personal data if the proposed processing is "likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)) (Binns 2017). Although processors and, in some cases, DPAs may assist here (Articles 28(3)(f), 35(4) and 36 GDPR), it is primarily for data controllers to undertake this assessment. At minimum, a DPIA must contain a systematic description of the envisaged processing, the purposes of the processing including (where appropriate) the legitimate interest pursued by the controller, the measures envisaged to ensure the protection of personal data and to demonstrate compliance with the GDPR, and an assessment of the necessity and proportionality of the processing operations and the risks to the rights and freedoms of individuals (Article 35(7)). DPIAs need not be published, although publication is encouraged by DPAs and accords with the general principles of transparency and accountability in Article 5 (Kosta 2020, p. 675). When a DPIA "indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk," the controller must consult the relevant DPA (Article 36(1)), which may then apply its powers under Article 58, which include banning (temporarily or permanently) the proposed processing (Article 58(2)(f)).

Although DPIAs are portrayed within the GDPR as an accountability measure placing primary responsibility for identifying and taking steps to safeguard against the risks of personal data processing on the data controller (Recital 84), they also serve as "early warning systems" to alert controllers and, indirectly, DPAs, to anticipated dangers that require mitigation (Kloza *et al.* 2017, p. 1). As such, DPIAs and their closely linked (but not fully commensurate), older counterpart, Privacy Impact Assessments (PIAs), superficially resemble earlier regulatory decision-making tools such as technology impact assessment, environmental impact assessment, and impact assessment of medical research (on this heritage, see Wright & De Hert 2012; Clarke 2009). But unlike these older tools, which were used by public agencies to inform their evaluation of specific regulatory options or linked to ethical approval schemes (for medical research), DPIAs are undertaken by the regulated organizations and seek to assess the risks arising from their proposed activities. This move to "self-assessment" by regulated organizations could enhance the regime's effectiveness, helping to elicit "buy-in" from data controllers and cultivate within them an organizational culture in which the risks associated with personal data collection and processing are taken seriously (Parker 2002). Yet there is a real danger that DPIAs will be largely perfunctory, box-ticking exercises, exhibiting yet another form for what Michael Power terms "rituals of verification" (Power 1997). This danger might be exacerbated by the DPIA's primary touchstone for evaluation, namely the risks to the "rights and freedoms of natural persons." This is an extremely broad yet abstract frame of reference that many organizations may find bewildering (see Section 3.3). At the same time, unpacking its numerous dimensions may end up inducing what Charles Raab memorably describes as "counterproductive snow-blindness brought about by the blizzard of detailed questions" (Raab 2020). Experience within the UK financial services sector indicates that the claimed benefits of meta-regulation depend on a number of optimistic assumptions, including an assumption that the interests of the regulated organizations to design and implement internal control systems are aligned with the goals of the regulator, and that the organizations themselves have sufficient competence to manage their own internal control systems effectively. As Julia Black has argued, the 2008 financial crisis vividly demonstrated both in the UK and elsewhere that these assumptions may not

be borne out in practice, with the result that meta-regulation proved to be little more than an indulgent form of "myth-based" regulation (Black 2012, pp. 1045–1048). There remains a real risk that DPIAs may follow a similar fate.

2.2.4. Ex ante versus ex post regulatory modalities

Summing up then, it is easy to understand why the GDPR has been criticized as complex and difficult to navigate, given the variety of mechanisms through which it is operationalized. Aggravating this difficulty is that the regime also cannot be easily characterized in terms of a long-standing distinction, drawn primarily by economists, between ex ante and ex post approaches to regulation, which is often regarded as a key indicator of the stringency of a regulatory regime. Ex ante regimes rely on a system of prior approval by a regulatory authority, while ex post regimes typically entail the legal promulgation of certain minimum standards that the regulated activity must meet, thereby allowing the activity to be undertaken without obtaining prior approval, provided that legally mandated standards are met. Although some early national data protection regimes in Europe entailed extensive licensing requirements (Bygrave 2014, p. 184), advance authorization is generally not required by the GDPR nor national data protection regimes within the EU. This may suggest that the GDPR relies on an ex post rather than an ex ante strategy of control, yet the preceding analysis demonstrates various of its mechanisms have an ex ante flavor, including "data protection by design and by default" (Article 25), DPIAs (Article 35) and "prior consultations" with DPAs in respect of certain "high risk" processing operations (Article 36). These mechanisms allocate the responsibility for establishing internal control and compliance management systems on data controllers and processors *before* they commence processing personal data, reflecting the GDPR's stronger emphasis on accountability. Yet the delegation of various ex ante regulatory responsibilities to data controllers has been a continuing source of uncertainty. Chief among these uncertainties is a lack of clarity concerning how to assess whether a proposed processing entails a "high risk" to fundamental rights, an issue to which our discussion now turns.

3. The role of fundamental rights and the relationship between rights and "risk"

For public lawyers and human rights advocates, one of the most significant features of the European data protection regime is the central place it accords to fundamental rights. Despite this centrality, the precise role of fundamental rights (or "human rights" as they are more commonly known) within the regime is not readily understood. The protection of fundamental rights is one of the animating motivations and policy objectives of the regime itself, and a crucial touchstone for the evaluation of proposed data-processing operations for the purposes of undertaking a DPIA. Although the concept of "risk" is familiar to regulatory governance scholars (particularly in the guise of "risk assessment," "risk management", and "risk-based regulation"), the role of fundamental rights in the design and implementation of regulatory governance regimes is not. Not only is the notion of a "risk to rights" unfamiliar within this literature, the linking of risk to fundamental rights as a vehicle for regulating the processing of personal data may appear contradictory given the dignitarian basis for fundamental rights (elaborated below), while risk assessment is traditionally inherently directed toward numerical assessments of the probability and severity of tangible harm. Accordingly, the following analysis seeks to subject the rights-risk nexus to critical scrutiny in order to suggest how the GDPR's concept of a "risk to rights" can be best understood in light of the jurisprudental nature of rights themselves. To do this, it is first necessary to clarify what fundamental rights are and why they matter.

3.1. What are fundamental rights?

Fundamental rights are abstract social constructs rather than tangible objects or natural phenomena that can be readily observed and quantified. They mark out protected spheres that seek to safeguard foundational, largely intangible *moral values* associated with the inherent dignity of persons, rather than concerned primarily with safeguarding individuals against tangible harms. Fundamental rights have peremptory moral force, and many are accorded special legal protection pursuant to regional and international human rights instruments, including the EU Charter of Fundamental Rights (CFR) and European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).[7] Properly understood, fundamental rights serve as moral boundary markers such that any unjustified interference with them is, by definition, a serious moral wrong (Dworkin 1977). More

recently, fundamental rights have acquired greater prominence in debates about the need to regulate and govern emerging technologies (Brownsword & Goodwin 2012, p. 225).

3.2. Fundamental rights protection as an underpinning policy objective

The protection of fundamental rights as one of the European data protection regime's animating policy objectives can be traced back to its historical origins and the emergence of information communication technologies (ICTs). When the regime's foundations were established, there was growing concern that the emergence and spread of ICTs and associated data processing posed potential threats to individual freedom and autonomy (Bygrave 2002, ch. 6). Burkert observed that the new ICTs were then radically expanding the volume and speed of information handling, vastly increasing the number of individuals affected by information processing, and rendering temporal and spatial distance almost irrelevant in the acquisition and distribution of informational power (Burkert 1981). Debate about the need for data protection was informed by experiences of totalitarianism (such as the Nazi regime's use of state record-keeping systems to identify Jews and other "undesirables") and fictional dystopias (such as Orwell's *Nineteen Eighty Four*), thus helping to infuse the European data protection framework with a distinctive fundamental rights character.

While personal computing, the emergence of the internet, and the widespread availability and take up of smart connected devices has become so commonplace that contemporary life without the efficiency and convenience of the networked digital economy has become almost unthinkable, their undeniable benefits can obscure the ways in which these technologies threaten to erode the social foundations upon which democratic freedom is rooted (Bartlett 2018). Hence, the dangers associated with personal data processing reach beyond a concern for fundamental rights understood in highly individualized terms (Cohen 2019). Although the protection of privacy has constituted an important dimension in the struggle for informational power between data subjects and those wishing to collect and process their personal data, many other interests – including personal autonomy, integrity, dignity, pluralism, and democracy – have also formed an integral part of the rationale and agenda of European data protection law (Bygrave 2002, pp. 134–136). These interests extend beyond individual goals of self-realization to the interests of society as a whole, particularly its character as a "deliberative democracy" (Simitis 1984; Schwartz 1995). Seen in this light, contemporary data protection law can be understood as analogous to environmental regulation: it seeks to protect the democratic "commons," that is, the moral, democratic, and cultural environment, as opposed to the natural, physical environment (Gellert 2015, pp. 11–12). By seeking to safeguard the collective social and cultural foundations which liberal democratic orders presuppose, and without which individual dignity, autonomy, and self-development would not be possible (Ferretti 2014; Mantelero 2016), the "fundamental rights" character and the justification for establishing a general regime of protection specifically concerned with regulating the processing of personal data becomes more apparent and compelling.

3.3. The turn to "risk-based" approaches to compliance with European data protection law

With this understanding of fundamental rights, we can now examine their relationship with the pronounced emphasis on "risk" and on risk management techniques introduced by the GDPR as part of the "accountability" obligations placed on data controllers to demonstrate compliance. This "risk-based" turn is, as described below, directly tethered to the protection of fundamental rights. Yet the relationship between risk and fundamental rights is poorly theorized in human rights scholarship generally,[8] and largely overlooked by regulatory governance scholars, who have tended to perceive rights in narrow terms, either as side constraints or as substantive goals of the regulatory endeavour, or as a vehicle through which private actors may vindicate a regulatory regime's underlying policy goals via litigation. Although data protection law scholars have begun to address this relationship in the context of the European data protection regime (see e.g. Quelle 2017; Gellert 2018; Gellert 2020), this work remains in its infancy and has often been informed by close textual analysis of the GDPR's provisions. The following discussion can be understood as complementing these analyses, by critically investigating the rights-risk nexus within the European data protection regime but at a different level of abstraction. We begin with the jurisprudential character of rights and draw on insights from regulatory governance studies concerned with risk regulation and risk management in order to enrich understanding of this potentially fraught relationship. At the same time, we offer an interpretation of how the

concept of a "risk to rights" can best be understood within the context of the GDPR's embrace of a "risk-based" approach.

3.3.1. What is meant by a "risk-based" approach to data protection?

Risk-based approaches to data protection are not new within informational privacy discourse. Yet with the exception of the work of Raphael Gellert and his colleagues who have analyzed how the concept of risk within the GDPR can be understood in light of concepts of risk analysis and risk management that are standard in professional risk evaluation (van Dijk *et al.* 2016; Gellert 2018; Gellert 2020), there is strikingly little analysis of what the concept of "risk" refers to in this context, or unpacking of what, exactly, is meant by a "risk-based" approach to data protection. Although Recital 75 GDPR opens with the statement that "(t)he risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage," the Regulation does not otherwise define the concept of "risk" nor attempt to identify precisely the risks with which it is concerned,[9] despite the meaning of "risk" and a "risk-based approach" being far from self-evident in this context. Particular care is needed due to the slippery and malleable way in which the term "risk" can be used (and abused) (Power 2004, pp. 13–14). Within conventional risk assessment methodologies (which draw heavily on a family of methods for the calculation of risk based in the statistical sciences), before any risk calculation can be made, it is first necessary to identify the relevant unwanted or adverse event (Power 2007; Allhoff 2009; Black 2010). For example, Allhoff offers an example of a new water purification technology that is toxic to fish which we wish to utilize in order to purify a lake in which 100 fish live. If we state a projection of 20%, this indicates that we expect to lose 20 fish, thereby expressing an expected outcome quantitatively in terms of some number of units lost. This is the approach adopted in standard professional risk assessment, which has the advantage of allowing risks to be quantitatively assessed, and this may help make them commensurable with benefits. Yet in the context of the GDPR these issues are frequently glossed over, which can readily lead to confusion and misunderstanding. In Allhoff's example, it is the risks *to the fish* that are the focus of analysis. Yet in regulatory governance scholarship, a distinction is drawn between "societal risk" (i.e. risks *to society* from a range of sources, including new technologies) on the one hand, and "institutional risk" on the other (i.e. risks posed to a *specific institution* arising from a particular activity or event), both of which must be assessed by regulatory agencies wishing to develop and implement "risk-based regulation" (Black 2005; Rothstein *et al.* 2006; Black 2012).

Who, then, are the relevant risk-bearers when the term "risk" is used in the context of the European data protection regime? And what are the relevant "unwanted events" to which the "risk" is intended to refer? Lynskey approaches this question by initially focusing on "privacy risks" faced by individuals and society, observing that there is no comprehensive taxonomy of such risks, while noting that "these harms are difficult to quantify" (Lynskey 2015, p. 86). Yet neither the concept of a "privacy risk" nor that of "harm" occupies a central place in the text of the GDPR. Gellert points out ambiguity in the wording of Article 35(1) in referring to the "risk to the rights and freedoms of natural persons", on the one hand, but requiring (if that risk is high) an assessment of the "impact…on the protection of personal data", and thereby seeks to identify what the Article 35(1) assessment actually requires in terms of both attention to compliance with the GDPR and/or the risks which the proposed processing poses to fundamental rights (Gellert 2018). Rather than engage in the conundrum which Gellert seeks to address, our concern is to understand the concept of a "risk to rights and freedoms of natural persons" in light of the place of fundamental rights within the GDPR and the jurisprudental nature of rights themselves and to consider how these might be reconciled with a "risk-based" approach to data protection. To this end, we suggest that the notion of "risk" and the relevant "risk-bearers" adopted in the European data protection regime are best understood in light of the above-cited text of Recital 75 GDPR (i.e. "(t)he risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage") and Recital 4, which provides:

> *This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and a fair trial, and cultural and religious and linguistic diversity.*

This indicates that an assessment must be made of the nature and magnitude of the potential threats posed by personal data processing to the *rights and freedoms of natural persons* recognized by CFR, and which need not sound in tangible damage. This requires a broad assessment of the possible range of interferences to the fundamental rights of natural persons generally, whether or not their personal data are the subject matter of the proposed data processing.[10]

3.3.2. Risks, rights, harms, and wrongs

Assuming that what must be assessed is the risk that a proposed personal data processing operation might violate the fundamental rights of natural persons (and not merely in their role as data subjects whose data are processed by the controller(s) in question), this immediately raises the question of whether the regime's risk-based approach is compatible with the regime's "fundamental rights character" (Lynskey 2015). Indeed, the very notion of a "risk" to fundamental rights seems problematic, given that the origins of risk assessment lie in statistical evaluation concerned with tangible harms that are directly quantifiable in mathematical terms (Allhoff 2009). Thus, from the perspective of constitutional and human rights scholarship and legal and moral philosophy, speaking in terms of "risks to rights" is inherently questionable because it potentially misconceives the very nature of rights and rights protection.[11] The language of risk and the methodologies of risk assessment might imply that fundamental rights violations can be quantified and measured in degrees, rather than recognizing the status of rights protection as critical moral boundary markers. Although when analyzing violations of fundamental rights, it is possible and meaningful to speak of different levels of culpability (e.g. particularly "egregious" moral wrongs, in which intentional violations are more culpable than unintentional violations), scale (i.e. whether only a few individuals are affected as opposed to whole populations), and magnitude (e.g. reading only one personal letter without permission in contrast to reading 5 years' worth of personal diaries), these variations do not imply that fundamental rights violations can be unproblematically ranked on a sliding scale from trivial to serious. A violation of a fundamental right is a serious moral wrong, *tout court*. Thus, attempts to evaluate potential violations of fundamental rights in terms of relative "risk" levels seem to fly in the very face of their jurisprudential structure and philosophical foundations as setting universal moral boundaries for which deviation cannot be countenanced except in narrowly defined circumstances, which are necessary and proportionate in a democratic society.

3.3.3. Reconciling a "risk-based approach" to data protection with respect for fundamental rights: The need for proportionate safeguards

How can this tension between the language and understanding of risk as a statistical construct and the discourse and jurisprudential structure of rights be reconciled? We suggest that the regime's concept of "risks to fundamental rights," which triggers the Article 35(1) obligation to undertake a data protection impact assessment can be best understood by considering first those proposed data-processing practices that present a *clear violation* of fundamental rights (e.g. a proposal to configure smart home assistants so that they record and analyze on a continuous basis all the interactions between the home's occupants to create detailed profiles of each occupant for the purposes of serving up targeted advertising). In our view, proposed processing operations that would, if implemented, *clearly* violate fundamental rights would also violate the regime's principle of "lawfulness, fairness, and transparency" and therefore cannot lawfully proceed,[12] while also serving as a benchmark for assessing less clear-cut potential interferences that are the main focus of Article 35. In contrast, proposed processing operations that could be regarded as "borderline" in that there is some uncertainty about whether they would, if implemented, constitute a violation of fundamental rights (perhaps because the proposed processing affects fundamental rights in a novel way or because it might threaten the democratic "commons" in which fundamental rights are anchored) can fall within the scope of Article 35(1) if the severity and probability of the threatened "risk" to fundamental rights are "high". In these "borderline" cases, a greater level of scrutiny, more demanding safeguards and appropriately greater caution is warranted before such proposed practices should be allowed to proceed (if at all). Hence the stringency of safeguards that data controllers must implement will vary in proportion to the severity and probability of the threatened "risk": the higher the risk that the processing will violate fundamental rights, the more stringent and the demanding the safeguards required to ameliorate such threats in order to comply with the GDPR's "data protection by design" requirements referred to at section 2.2.2 above (Gellert 2015; Quelle 2017). So understood, the risk-based approach required by the GDPR necessitates that the data controller undertake a contextual "fundamental rights risk assessment" in order to identify the appropriate

level of stringency of the technical and organizational measures that must be adopted to guard against those risks from materializing, also as required by Articles 24 and 25. This interpretation is consistent with the line taken by the Article 29 Working Party's description of a risk-based approach as a "scalable and proportionate approach to compliance" (Article 29 Working Party 2017, p. 2).

It is important to recognize, however, that this "risk-based approach" is quite different and distinct from the concept of "risk-based regulation" that has been advocated as a strategic approach to enforcement by a number of regulatory agencies and which has been subject to critical examination by regulatory governance scholars (Black 2005; Black 2012; Beaussier *et al.* 2016). Unlike risk-based approaches to data protection, which are concerned primarily with the obligations of the *regulated organizations*, "risk-based regulation" is a strategy which *regulated enforcement officials* are exhorted to adopt in order 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. In other words, the two phenomena are entirely different and distinct, despite the confusing similarity in the language and terminology used to describe them.

3.3.4. Operationalizing risk-based approaches to data protection

Our analysis highlights the challenges of integrating the language and discourse of risk, which is rooted in the statistical sciences and more recently translated into the language of organizational management to assist organizations in strategic planning, with the language and conceptual structure of fundamental rights, understood as boundary markers which carve out moral interests of vital human importance. By integrating insights from regulatory governance studies concerned with the management of risk with legal scholarship concerning the nature, structure, and peremptory force of rights alongside insights from data protection law experts, we have obtained a clearer account of the relationship between risk and rights. Yet data controllers who must carry out these assessments may be ill-equipped to do so for at least four partially overlapping reasons. First, the fundamental rights protected under the EU Charter rest on conceptual abstractions which those not well versed in the discourse and practice of fundamental rights may struggle to comprehend. Secondly, controllers are required to consider fundamental rights of individuals generally, rather than merely the rights of data subjects directly implicated by the proposed processing. Thirdly, many private and non-governmental organizations are unlikely to have any significant experience in understanding the nature and scope of fundamental rights protection since the chief instruments of such protection, such as the ECHR and CFR, are primarily applied as obligations on state organs and their application to private actors has been slow, fragmented and inconsistent (Gerards 2019, pp. 136-159; Frantziou 2019). Fourthly, although the GDPR lists three concrete examples of high-risk data-processing operations (Article 35(3)), it provides guidance predominantly on so-called toxicological factors (i.e. sources of risk), leaving epidemiological factors (i.e. consequences of harm) and methodologies for assessing harm largely undelineated (Gellert 2020, pp. 215ff). Data controllers will invariably want more concrete guidance concerning how, precisely, to undertake a fundamental rights risk assessment for the purposes of undertaking a GDPR-compliant DPIA, particularly given the prospect of hefty sanctions for failure to do so when required (Article 83(4)(a)). Although DPAs have issued fairly extensive guidance on DPIA and "high risk" processing (Article 29 Working Party 2017)—and, indeed, must do so pursuant to Article 35(4) GDPR—claims persist that the precise criteria for conducting a proper DPIA, and the actions which must follow, lack clarity, and that DPAs' respective policies on point are sometimes inconsistent (Multistakeholder Expert Group 2019, pp. 13, 15; European Commission 2020b, p. 5). It is also reported that this lack of clarity has resulted in some companies adopting a conservative, "risk-adverse" approach whereby *all* proposed processing is subject to a DPIA (Multistakeholder Expert Group 2019, p. 15). This undermines the efficiency gains that risk-based strategies sought to generate. Yet it also reveals the pivotal role of DPAs not only in ensuring that DPIAs are properly carried out, but also in shaping the content, contours and, ultimately, the success of the regime in fulfilling its policy objectives. Hence, it is to the institutional dimensions of the regime and the role of DPAs and courts in monitoring and enforcing the GDPR that we now turn.

4. Institutional dimensions

4.1. The status, role and powers of data protection authorities (DPAs)

A significant feature of the European data protection tradition is its reliance on independent, *sui generis* administrative agencies: DPAs (referred to in the GDPR as "supervisory authorities"), for monitoring and enforcement. They are an integral part of the EU data protection regime, and their establishment is a constitutional requirement under EU primary law,[13] forming an essential part of the individual's fundamental right to data protection.[14] DPAs are critical contributors in ratcheting up the EU's regulatory capacity (Newman 2008) in the data protection arena (relative to the equivalent capacity of non-European states), thereby bolstering the "Brussels Effect" (Bradford 2012; Bradford 2020).[15] Yet as Raab and Szekely (2017, p. 421) note:

> *DPAs play a major role in arbitrating the degree of information privacy that we enjoy as a fundamental right. Their institutional arrangements, provenance, independence, and performance are crucial to that enjoyment, but are less frequently, less systematically, and less comparatively investigated than many of the other components of data protection regimes.*[16]

European DPAs are a distinctive type of independent regulatory agency (IRA) for they regulate both private sector bodies and state agencies (Schütz 2012). Accordingly, EU law places a very high premium on their independence, which is constitutionally required under EU primary law, strictly construed by the CJEU,[17] and reflected in the GDPR itself.[18] Although this has potentially problematic implications for DPAs' accountability and legitimacy in respect of the checks and balances built into the constitutional architecture of pluralist democracies, the CJEU has emphasized that DPAs are nevertheless subject to basic boundaries set by constitutional law and are not excluded from judicial review.[19]

DPAs are multi-taskers: Article 57 GDPR enumerates over 20 tasks they must undertake, including the generic task of "fulfil[ling] any other tasks related to protection of personal data". To discharge their mandate, they enjoy numerous powers (Article 58 GDPR enumerates 26 of these) which are largely discretionary in nature, a characteristic trait which socio-legal scholars have long identified as necessary for administrative authorities to operate effectively within all modern legal systems (Galligan 1986). These broad discretionary powers apply to the exercise of DPA's enforcement functions, thereby conferring upon them considerable interpretative leeway in administering and applying the GDPR's requirements. This leeway is bolstered by the dearth of case law establishing the authoritative meaning of specific legislative provisions (Bygrave 2014, p. 179). Especially noteworthy is the pan-European promulgation of administrative guidelines setting out how DPAs propose to interpret the relevant law and exercise their enforcement discretion. This facility was long exercised by the so-called Article 29 Working Party pursuant to the former DPD but has now devolved to the European Data Protection Board (EDPB) pursuant to Articles 68–70 GDPR. Like its predecessor, the Board is composed predominantly of representatives of the EU member state DPAs. Although the opinions of these bodies are advisory only, they are accorded considerable weight by the broader data protection community and the judiciary (Bygrave 2014, pp. 174–175). We return to this interpretative function further below.

4.2. DPAs and the politics of regulation

As a result of their extensive mandate and powers, DPAs enjoy considerable discretionary authority. However, some of their mandated tasks create internal tensions, particularly between their "policy or leadership-oriented tasks" (Hijmans 2020, p. 934) that involve, inter alia, promoting awareness of data protection (see particularly Article 57(1)(b) and 57(1)(d) GDPR) and that of unbiased interpretation, application, and enforcement of the law. DPAs vary considerably in how they strike the balance between these two tasks.[20] The scope of their discretionary power, and the inevitable normative trade-offs that the exercise of that power entails in specific contexts, point to larger dilemmas and contradictions that have plagued independent regulatory agencies (IRAs) more generally. In particular, regulatory governance scholars have highlighted difficulties in reconciling the extensive power and functions of IRAs with their formal independence from a state's democratically elected representatives and the concomitant challenges this presents for their accountability and legitimacy. IRAs have considerable influence in determining the distribution of benefits and burdens between different groups and stakeholders in discharging their regulatory duties, yet they lack a direct democratic mandate. Hence, scholars have theorized

about how this legitimacy deficit can be overcome or at least reduced: typically either by reference to expertise on the one hand (Majone 1996), or democratic participation on the other (Morgan & Yeung 2007, ch. 5; Black 2008; Rahman 2011). DPAs tend to rely predominantly on their expertise to shore up their legitimacy, underpinned by their bespoke and largely exclusive remit over an area of law that confers upon them a body of knowledge that is relatively arcane to others. The minor, if not marginal, involvement of national courts across many jurisdictions in interpreting data protection laws reinforces DPAs' authoritative position as the primary "disambiguators" of data protection norms. While this interpretative role may bolster their status and power, it is a double-edged sword. If DPAs fail to offer clear and timely guidance that satisfies the demands of wider society, they will be vulnerable to criticism. For example, the EU Council's recent evaluation of the GDPR's application acknowledged DPAs' important role in operationalizing the GDPR, welcomed the increase in their activities (linked to exercise of their new powers) and the "significantly increased allocation of resources to them in many Member States" (EU Council 2019, p. 4), yet it also stated:

> *the Council deems that controllers and processors need more clarification and guidance from the supervisory authorities and the EDPB. The Commission's upcoming evaluation report should also highlight the broad need for practical guidelines and other suitable means to meet this need of the EU. (EU Council 2019, p. 6)*

This clear expression of impatience is echoed by industry representatives who have criticized the EDPB not just for failing to provide timely guidance but also, in some cases, clear and consistent guidance (Multistakeholder Expert Group 2019, pp. 4–6). These shortcomings are due not merely to the scale of the GDPR's textual ambiguities but also to DPAs' lack of capacity. Many DPAs have long suffered from chronic shortages in staff and other resources (Flaherty 1989, p. 404) although significant variations exist among them (EDPB 2019, pp. 7, 10–11; Raab & Szekely 2017; European Commission 2020b, p. 6). The Irish DPA, for example, has long been regarded as especially "undernourished," particularly given that it has digital Goliaths such as Facebook and Amazon on its home turf and is thus meant to take the lead in undertaking the relatively complex and demanding task of auditing their operations and ensuring they comply with the law – a point indirectly acknowledged by the European Commission in its first review of the GDPR's operations (European Commission 2020b, p. 6).

The resource shortage compromises DPAs' ability to fulfill their wide-ranging mandate under the GDPR (Taylor 2020), including their responsiveness to demands for clear and timely guidance on the meaning of its provisions. Yet even if DPAs do deliver such guidance, regulatees might be inclined to regard it as unfairly influenced by DPAs' pro-privacy mandate (Bygrave 2014, p. 4), thereby threatening the perceived legitimacy of the guidance, DPAs, and even the regime itself. The risk is exacerbated by long-running perceptions on the part of many governments and businesses that DPAs are, in effect, "flies in the ointment" that get in the way of governments' and businesses' ability to fulfill their respective legitimate goals efficiently (Flaherty 1989; Cohen 2013). Julie Cohen astutely observes that "privacy has an image problem" in the sense that it is often regarded as "anti-progressive, overly costly, and inimical to the welfare of the body politic" (Cohen 2013, p. 1904). Much the same can be said for DPAs. But this perception does not apply uniformly across the board. While difficult to document, our impression is that some DPAs are commonly regarded as relatively friendly to the needs of government and business, and others as relatively hostile. The Irish and UK authorities are examples of the former, whereas French, Spanish, and German authorities are examples of the latter.

4.3. The role of courts

Courts occupy a different position, enjoying greater independence from political pressures than DPAs. They do not face demands to issue swift guidance, nor are they so vulnerable to perceptions of pro-privacy bias. Yet they inevitably shape the direction and focus of jurisprudence as cases are brought before them; hence some norms receive greater judicial attention while others are marginalized or overlooked. This is evident in the CJEU's workload, including requests for preliminary rulings in a relatively large number of cases concerning fundamental rights of privacy and data protection but very few cases concerning freedom of expression. This might suggest that the CJEU favors the former rights over the latter, which its ruling in the famous *Google Spain* case (in which the so-called "right to be forgotten" was first established) may have reinforced. Yet the CJEU and the European

Court of Human Rights (ECtHR) command widespread respect in their respective jurisdictions. Both have been instrumental in shoring up the walls of data protection against the relentless pressure of business and government interests in processing ever greater amounts of personal data for self-interested ends, and have thereby offered "lifelines of support" to DPAs. Indeed, European DPAs and the CJEU (and to a more limited degree the ECtHR) have developed a functionally close, almost symbiotic relationship. As Bieker observes, the CJEU "has consistently strengthened the role of the authorities in its jurisprudence and in turn expects them to use their independence to fulfill their role as guardians of individual rights with regard to privacy and data protection" (Bieker 2017, p. 138). At the same time, some have pointed to a recent tendency whereby civil society groups with a pro-privacy agenda are increasingly going straight to the courts (first at the national level then at the European level) to enforce or test the rules of the GDPR, and largely bypassing DPAs in the process. This is partly a result of a perception that DPAs ultimately do not have the same power or punch as the courts in enforcing the law or in delivering compensation to complainants, and partly a reaction to DPAs' resource problem identified above (Manancourt 2020).

Arguably the CJEU's most important role has been to temper, if not entirely debunk, claims that data protection law is merely what Aubert (1966) termed "symbolic legislation," that is, legislation designed to give the impression of creating change (e.g. in the form of new rights or protections) but serving predominantly to uphold the status quo. This charge was leveled at the FIPPs several decades earlier (Rule *et al.* 1980), undermining data protection law's claims to a "higher" normative legitimacy. Ground-breaking judicial decisions such as those in *Google Spain*, *Digital Rights Ireland*, and *Schrems I*—which, in the name of privacy and data protection, demonstrate that the regime is neither meaningless nor toothless—help keep those claims alive. Accordingly, the CJEU plays a pivotal role in determining the balance between the twin goals upon which the European data protection regime was originally founded: safeguarding fundamental rights *and* fostering a thriving data economy within the single European market. The Court has tilted the balance in favor of the former goal – a shift reflected subtly in the GDPR (Hijmans 2020) – without fully jettisoning the latter goal. Where precisely the balance is struck by the CJEU will inevitably fluctuate over time in light of changing social, political, technical, economic and moral concerns and contexts. Yet the regime will continue to retain the duality of its animating objectives, particularly given the ongoing emphasis by the Commission and Council on the regime's importance for fostering a vibrant "European data economy" and the uptake of new ICTs (see e.g. European Commission 2020a).

5. Conclusion

The preceding analysis has highlighted the multi-faceted, complex and somewhat opaque character of the European data protection regime, including its reliance on a variety of novel regulatory techniques and broadly framed norms. It is therefore not surprising many find the regime bewildering and struggle to understand what it requires in practice. By applying insights from both regulatory governance literature on the one hand and from legal scholarship concerning fundamental rights, data protection and the challenges of rule-drafting and interpretation on the other, we have sought to "demystify" two key aspects of the regime that have been a source of misunderstanding and confusion: the regime's regulatory architecture and the role of fundamental rights in the regime's emphasis on "risk-based" approaches to compliance. In so doing, we have demonstrated how an integration of these two scholarly perspectives can offer an enriched account of the GDPR understood as a regulatory regime, and offers a fruitful methodological approach that can be applied for examining regulatory regimes more generally.

Our examination of the GDPR's architecture suggests that its reliance on a variety of techniques can be understood as a strategic mix of complementary regulatory policy tools and modalities, resonating with those who advocate "smart" regulatory approaches that are claimed to be more effective and less intrusive in facilitating the achievement of regulatory policy objectives (Gunningham & Grabosky 1998). It also demonstrates that the regime which the GDPR establishes is not readily characterized in terms of the kinds of binary distinctions often relied on in attempts to classify regulatory norms, modalities and techniques. The GDPR's role in regulating the processing of personal data is far more nuanced and sophisticated than simply promulgating a series of commands to be complied with on pain of state-enforced punitive sanction for violation, revealing the fallacy of exclusively equating the law's role in regulation with "command-and-control" regimes as is commonly believed. It also reveals how pitching "code" in opposition to "law" as competing modalities of control rests on a false

dichotomy: code can be harnessed in the service of regulatory objectives imposing legal duties on the regulated organizations to hard-wire safeguards into their information systems and organizational practices. Nor are the core data protection principles lying at the foundation of the GDPR easily characterized as "process-based" or "outcome-based" in orientation, even though they are generally framed as largely open-ended "principles" rather than highly detailed rules. Accordingly, the structure and intended operation of the regime demonstrates why ongoing debates about the regulation of the tech industry generally, and AI in particular, that have been portrayed as a choice between heavy-handed command-and-control regulation, or voluntary industry self-regulation on the other, are misleading and wrong-headed. Although the EU data protection regime is both technical and complex, drawing upon a range of techniques that combine both ex ante and ex post approaches, there is an underlying method to its apparent madness, underpinned by an overarching orientation that is primarily preventative: seeking to anticipate and prevent the unlimited collection and repurposing of personal data in order to reduce the dangers that might arise in the absence of any up-front restrictions. Hildebrandt provides an apt metaphor for this endeavor, likeningit to Odysseus's strategy of tying himself and his crew to the mast to prevent them responding to the Sirens' call, thereby "enabling them to resist the overweaning temptation to gather more and more data and use it for more and more intrusive purposes and applications that will ultimately lead to downfall and destruction" (Hildebrandt 2015, p. 194).

This preventative orientation is reflected in the regime's new emphasis on "risk-based" approaches to compliance. Yet the jurisprudential character of fundamental rights as critical moral boundary markers associated with the inherent dignity of persons may appear conceptually incompatible with quantitative understandings of risk originating in the statistical sciences upon which professional risk assessment methodologies are rooted. By seeking to reconcile insights from regulatory governance studies concerned with the management of risk and risk-based regulation with legal scholarship concerning the nature, structure and peremptory force of rights, we have suggested how the relationship between risk and rights reflected in the regime's risk-based approach to compliance can best be understood so as to preserve the peremptory force of fundamental rights protection. At the same time, the task imposed on data controllers of assessing the risk that their proposed processing might pose to fundamental rights is neither simple nor straightforward: the GDPR assumes that they understand what fundamental rights are, and have the capacity to undertake a meaningful evaluation of whether and in what ways personal data processing operations might threaten those rights. However, such knowledge and competence is unlikely to be widely held by data controllers, who are likely to need expert advice (and to shoulder the concomitant costs and compliance burden such advice entails) to dispel their bewilderment.

Part of this compliance burden arises from continuing uncertainty about how specific provisions of the GDPR are expected to be operationalized in practice. The GDPR's provisions on DPIAs exemplify the broad and open-textured character of many of the GDPR's norms, often generating significant uncertainty for those legally bound to comply with them on pain of very significant sanctions. This underlines the critical role of DPAs in offering swift, clear and consistent guidance that regulatees can rely on in seeking to comply with its terms. But the wide interpretative discretion bestowed upon DPAs is, for them, a mixed blessing, particularly given their constitutionally protected independence from democratically elected representatives and their vulnerability to claims of pro-privacy bias. In particular, the need to mediate the tension between the regime's twin animating motivations in protecting fundamental rights and in fostering a flourishing data economy within the European single market will invariably be shaped by the way in which DPAs discharge their mandate to enforce the regime. Although these dual policy objectives are a source of interpretative tension, they may also be a source of strength, providing the regime with at least two legs upon which to stand and which are likely to appeal to quite different sets of interests that are frequently in conflict.

Ultimately, European courts have the final word in providing an authorative interpretation of the regime's requirements, and they have consistently demonstrated the importance of taking fundamental rights seriously when adjudicating disputes concerning the regime's requirements. Uncertainty associated with the meaning of the regime's norms may be undesirable and burdensome in the short term, particularly for regulated firms committed to complying with its norms. Nonetheless, it may well prove invaluable in the longer term. Given both the complexity and sophistication of technological systems through which personal data are processed and its insights applied in contemporary practice and the rapid pace of continuing innovation in digital data-driven technologies, the regime's focus on personal data processing as the critical trigger for the regime's operative provisions may provide greater resilience and durability in the face of technological advancement. This "technology-neutral"

approach avoids singling out specific types of technological systems or instruments which may rapidly become obsolete. In other words, although the current level of interpretative uncertainty may be undesirable and a source of significant mystification during the regime's infancy, this interpretative openness may be needed to "future-proof" the regime so that its meaning and requirements can evolve as technological innovation continues its rapid onward march (Black 1997).

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study

Endnotes

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

[2] Various interrelated criticisms are leveled at the regime's growing complexity and opacity (see e.g. Koops 2014; Bygrave 2017a), a putative mismatch between its basic principles and conceptual assumptions on the one hand and the realities of cloud computing platforms, online social networks, and "data hungry" machine-learning techniques on the other (see e.g. Mayer-Schönberger & Cukier 2013; Zarsky 2017), tensions between its "risk-based" approach and its commitment to safeguarding fundamental rights (see e.g. Lynskey 2015; Quelle 2017), and endemic weaknesses in the capacity of data protection authorities (DPAs) to carry out their monitoring, guidance, and enforcement duties (see e.g. Taylor 2020).

[3] The term "controller" denotes the person or organization that determines – or co-determines – the means and purposes of data processing: see further Article 4(7) GDPR.

[4] In relation to assessments of fire safety, see Spinardi 2019.

[5] Under the GDPR, the level of administrative fines has increased to a maximum of €20 million or 4% of an undertaking's annual turnover (Article 83(5)).

[6] For a discussion of experience with voluntary certification initiatives concerning environmental and labor standards, and potential lessons for certification mechanisms for AI systems, see Matus and Veale (2021) this volume.

[7] Kosta, however, argues that the protection of human rights afforded by the ECHR may be inadequate to address the use of secret algorithmic surveillance in light of the European Court on Human Rights' insistence upon the need for a specific identifiable "victim" who can claim human rights protection: Kosta (2021), this volume.

[8] Some of Therese Murphy's work in the field of human biotechnology in the first decade of the 21st century is a notable exception: Murphy 2009; Murphy and Whitty (2009).

[9] The DPIA guidelines issued by EU member state DPAs under the aegis of the former Article 29 Working Party (now European Data Protection Board) describe a series of "risk factor"' associated with personal data processing, rather than clarifying the nature of the underlying "risk" (Article 29 Working Party 2017).

[10] See also Article 35(7)(b) GDPR which states that the assessment required pursuant to Article 35(1) must include measures envisaged to address risks, "taking into account the legitimate rights and interests of data subjects and *other persons* (emphasis added)."

[11] Quelle (2017) raised a related but different problem arising at the intersection of rights and "risk-based" approaches to data protection, focusing on whether the risk-based approach required by the GDPR is consistent with the legal rights of data subjects set out in the GDPR. This question is beyond the scope of our inquiry.

[12] Quelle observed that the GDPR does not impose an explicit, self-standing obligation to protect individuals against risks to their rights and freedoms, in the absence of any duty to mitigate risk, with the obligation in Articles 24–25 stated as requiring controllers to "take risks into account." Hence, substantive protection must be grounded in the independent data protection principles, per Quelle 2017.

[13] See Article 8(3) CFR and Article 16(2) of the Treaty on Functioning of the European Union.

[14] See too Recital 117 GDPR.

[15] The "Brussels Effect" is a term coined by Bradford (2012) to denote the way(s) in which relatively strict EU rules have shaped policy development in areas outside Europe, leading to "Europeanization" of numerous norms across the globe. This effect is measured not just in terms of legislative change but also in terms of what corporate boardrooms around the world view as the "gold standard" to guide or otherwise shape their behavior.

[16] David Flaherty's landmark comparative analysis of the challenges facing the early DPAs of the Federal Republic of Germany, France, Canada, and Sweden (Flaherty 1989) is a notable exception, but it stems from the 1980s.

[17] See for example *European Commission v. Federal Republic of Germany*, Case C-518/07, judgment of 9 March 2010 (Grand Chamber).

[18] See especially Article 52(1) GDPR requiring that supervisory authorities "shall act with complete independence."

[19] *European Commission v. Federal Republic of Germany*, Case C-518/07, judgment of 9 March 2010 (Grand Chamber), paras. 39–42.

[20] For instance, Jóri (2015) detects that while advocacy is increasingly embraced by the European Data Protection Supervisor (EDPS), some national DPAs (primarily in Eastern Europe) show an opposite approach and have gone over to becoming "mere" enforcers of law, thus engendering a "technical" rather than "political" dimension to the European data protection regime.

References

Allhoff F (2009) Risk, Precaution, and Emerging Technologies. *Studies in Ethics, Law and Technology* 3(2) Article 2.

Article 29 Working Party (2017). 'Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679' (WP 248 rev.01, as last revised and adopted on 4 October 2017).

Aubert V (1966) Some Social Functions of Legislation. *Acta Sociologica* 10, 98–120.

Baldwin R, Lodge M, Scott C (2010) *Oxford Handbook of Regulation*. Oxford University Press, Oxford.

Bartlett J (2018) *The People vs Tech*. Penguin, London.

Bayamlıoğlu E (2021) The Right to Contest Automated Decisions under the GDPR. *Regulation & Governance* . https://doi.org/10.1111/rego.12391.

Beaussier AL, Demeritt D, Griffiths A, Rothstein H (2016) Accounting for Failure: Risk-based Regulation and the Problems of Ensuring Healthcare Quality in the NHS. *Health, Risk & Society* 18(3–4), 205–224.

Bemelmans-Videc ML, Rist RC, Vedung E (eds) (1998) *Carrots, Sticks & Sermons: Policy Instruments & Their Evaluation*. Transaction Publishers, New Brunswick N.J.

Bieker F (2017) Enforcing Data Protection Law – The Role of the Supervisory Authorities in Theory and Practice. In: Lehmann A, Whitehouse D, Fischer-Hübner S, Fritsch L, Raab C (eds) *Privacy and Identity Management: Facing up to Next Steps*, pp. 125–139.Springer, Dordrecht.

Binns R (2017) Data Protection Impact Assessments: A Meta-Regulatory Approach. *International Data Privacy Law* 7, 22–35.

Black J (1997) *Rules and Regulators*. Clarendon Press, Oxford.

Black J (2005) The Emergence of Risk-based Regulation and the New Public Risk Management in the United Kingdom. *Public Law*, 512–548.

Black J (2008) Constructing and Contesting Legitimacy and Accountability in Polycentric Regulatory Regimes. *Regulation & Governance* 2(2), 137–164.

Black J (2010) The Role of Risk in Regulatory Processes. In: Baldwin R, Cave M, Lodge M (eds) *The Oxford Handbook of Regulation*. Oxford University Press, Oxford Chapter 14.

Black J (2012) Paradoxes and Failures: 'New Governance' Techniques and the Financial Crisis. *Modern Law Review* 75(6), 1037–1063.

Black J (2014) Learning from Regulatory Disasters. *Policy Quarterly* 10, 3. https://doi.org/10.26686/pq.v10i3.4504.

Black J, Hopper M, Band C (2007) Making a Success of Principles-based Regulation. *Law and Financial Markets Review* 1(3), 191–206.

Bradford A (2012) The Brussels Effect. *Northwestern University Law Review* 107, 1–67.

Bradford A (2020) *The Brussels Effect*. Oxford University Press, Oxford.

Braithwaite J (2001) Rules and Principles: A Theory of Legal Certainty. *Australian Journal of Legal Philosophy* 27, 47–82.

Brownsword R, Goodwin M (2012) *Law and the Technologies of the Twenty-first Century*. Cambridge University Press, Cambridge.

Burkert H (1981) Institutions of Data Protection – An Attempt at a Functional Explanation of European National Data Protection Laws. *Computer Law Journal* 3, 166–188.

Burkert H (1988) The Law of Information Technology – Basic Concepts. *Datenschutz und Datensicherung*, 383–387.

Bygrave LA (2002) *Data Protection Law: Approaching its Rationale, Logic and Limits*. Kluwer Law International, The Hague.

Bygrave LA (2014) *Data Privacy Law*. Oxford University Press, Oxford.

Bygrave LA (2017a) Hardwiring Privacy. In: Brownsword R, Scotford E, Yeung K (eds) *The Oxford Handbook of Law, Regulation, and Technology*, pp. 754–775.Oxford University Press, Oxford.

Bygrave LA (2019) Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision-Making. In: Yeung K, Lodge M (eds) *Algorithmic Regulation*, pp. 246–260.Oxford University Press, Oxford.

Bygrave LA (2020) Article 25. Data Protection by Design and by Default. In: Kuner C, Bygrave LA, Docksey C (eds) *The EU General Data Protection Regulation (GDPR): A Commentary*, pp. 571–581.Oxford University Press, Oxford.

Clarke R (2009) Privacy Impact Assessment: Its Origins and Development. *Computer Law & Security Review* 25, 123–135.

Coglianese C (2017) The Limits of Performance-based Regulation. *University of Michigan Journal of Law Reform* 50, 525–563.

Cohen JE (2013) What Privacy Is For. *Harvard Law Review* 126, 1904–1933.

Cohen JE (2019) Turning Privacy Inside Out. *Theoretical Inquiries in Law* 20(1), 1–32.

Diver C (1983) The Optimal Precision of Legal Rules. *Yale Law Journal* 93, 65–109.
Dworkin R (1977) *Taking Rights Seriously*. Duckworth, London.
EU Council (2019). Council Position and Findings on the Application of the General Data Protection Regulation (GDPR). 14994/1/19 REV 1. [Last accessed 19 April 2021.] Available from URL: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/en/pdf.
European Commission (2020a). White Paper: On Artificial Intelligence – A European approach to excellence and trust. COM (2020) 65 final (19 February 2020).
European Data Protection Board (EDPB) (2019). First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities. [Last accessed 21 April 2021.] Available from URL https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf.
European Commission (2020b). Communication: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection' Regulation. COM(2020) 264 final (24 June 2020).
Ferretti F (2014) Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights? *Common Market Law Review* 51, 843–868.
Flaherty DH (1989) *Protecting Privacy in Surveillance Societies*. University of North Carolina Press, Chapel Hill and London.
Ford C (2010) Principles-based Securities Regulation in the Wake of the Global Financial Crisis. *McGill Law Journal* 55, 257–307.
Frantziou E (2019) *The Horizontal Effect of Fundamental Rights in the European Union: A Constitutional Analysis*. Oxford: Oxford University Press.
Galligan DJ (1986) *Discretionary Powers in the Legal Order*. Oxford University Press, Oxford.
Gellert R (2015) Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative. *International Data Privacy Law* 5, 3–19.
Gellert R (2018) Understanding the Notion of Risk in the General Data Protection Regulation. *Computer Law and Security Review* 34, 279–288.
Gellert R (2020) *The Risk-based Approach to Data Protection*. Oxford University Press, Oxford.
Gerards J (2019) *General Principles of the European Convention on Human Rights*. Cambridge: Cambridge University Press.
Gunningham N, Grabosky P (1998). *Smart Regulation: Designing Environmental Policy*. Oxford: Oxford University Press.
Hijmans H (2020) Article 57. Tasks. In: Kuner C, Bygrave LA, Docksey C (eds) *The EU General Data Protection Regulation (GDPR): A Commentary*, pp. 927–938.Oxford University Press, Oxford.
Hildebrandt M (2011) Legal Protection by Design: Objections and Refutations. *Legisprudence* 5, 223–248.
Hildebrandt M (2015) *Smart Technologies and the End(S) of Law*. Edward Elgar, Cheltenham.
Hood C, Rothstein H, Baldwin R (2001) *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford University Press, Oxford.
Jóri A (2015) Shaping vs Applying Data Protection Law: Two Core Functions of Data Protection Authorities. *International Data Privacy Law* 5, 133–143.
Koops B-J (2014) The Trouble with European Data Protection Law. *International Data Privacy Law* 4, 250–261.
Kloza D, van Dijk N, Gellert R, Böröcz I, Tanas A, Mantovani E, Quinn P (2017) Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals d.dpia.law Policy Brief 1, 1–4. [Last accessed 21 April 2021.] Available at URL http://virthost.vub.ac.be/LSTS/dpialab/images/dpialabcontent/dpialab_pb2017-1_final.pdf.
Kosta E (2020) Article 35. Data Protection Impact Assessment. In: Kuner C, Bygrave LA, Docksey C (eds) *The EU General Data Protection Regulation (GDPR): A Commentary*, pp. 665–679.Oxford University Press, Oxford.
Kosta E (2021) Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights. *Regulation & Governance*. https://doi.org/10.1111/rego.12331.
Lessig L (1999) *Code and Other Laws of Cyberspace*. Basic Books, New York.
Lessig L (2006) *Code Version 2.0*. New York: Basic Books.
Lodge M, Wegrich K (2012) *Managing Regulation*. Palgrave Macmillan, London.
Lynskey O (2015) *The Foundations of EU Data Protection Law*. Oxford University Press, Oxford.
Majone GD (1996) Regulatory Legitimacy. In: Majone GD (ed) *Regulating Europe*, pp. 284–301.Routledge, London.
Manancourt V (2020) Have a GDPR Complaint? Skip the Regulator and Take it to the Court. *Politico*, [Last accessed 30 August 2020.] Available from URL: https://www.politico.eu/article/have-a-gdpr-complaint-skip-the-regulator-and-take-it-to-court/.
Mantelero A (2016) Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection. *Computer Law & Security Review* 32, 238–255.
Matus K, Veale M (2021) Certification Systems for Machine Learning: Lessons from Sustainability. *Regulation & Governance* Special Issue "Algorithmic Regulation", edited by L Ulbricht and K Yeung.
Mayer-Schönberger V, Cukier K (2013) *Big Data: A Revolution that Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt, Boston/New York.
McBarnet D, Whelan C (1991) The Elusive Spirit of the Law: Formalism and the Struggle for Legal Control. *Modern Law Review* 54, 848–873.
Morgan B, Yeung K (2007) *An Introduction to Law and Regulation*. Cambridge University Press, Cambridge.
Multistakeholder Expert Group (2019). Contribution of the Multistakeholder Expert Group to the Stock-taking Exercise of June 2019 on One Year of GDPR Application [Last accessed 13 June 2019.] Available from URL: https://ec.europa.eu/commission/sites/beta-political/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf.

Murphy T (2009) Technology, Tools and Toxic Expectations: Post-publication Notes on New Technologies and Human Rights. *Law Innovation and Technology* 1(2), 181–202.
Murphy T, Whitty N (2009) Is Human Rights Prepared? Risk, Rights and Public Health Emergencies. *Medical Law Review* 17 (2), 219–244.
Newman AL (2008) *Protectors of Privacy: Regulating Personal Data in the Global Economy*. Cornell University Press, Cornell.
Ogus A (2004) *Regulation – Legal Form and Economic Theory*. Hart Publishing, Oregon.
Parker C (2002) *The Open Corporation: Effective Self-Regulation and Democracy*. Cambridge University Press, Cambridge.
Power M (1997) *The Audit Society: Rituals of Verification*. Oxford University Press, Oxford.
Power M (2004) The Risk Management of Everything. *The Risk Management of Everything: Rethinking the Politics of Uncertainty*. Demos, London.
Power M (2007) *Organised Uncertainty*. Oxford University Press, Oxford.
Quelle C (2017) The "Risk Revolution" in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too. In: Leenes R, van Brakel R, Gutwirth S, De Hert P (eds) *Data Protection and Privacy: The Age of Intelligent Machines*, pp. 33–62.Hart Publishing, Oxford.
Raab C (2020) Information Privacy, Impact Assessment, and the Place of Ethics. *Computer Law & Security* 37, 105404.
Raab C, Szekely I (2017) Data Protection Authorities and Information Technology. *Computer Law & Security Review* 33, 421–433.
Rahman KS (2011) Envisioning the Regulatory State: Technocracy, Democracy and Institutional Experimentation in the 2010 Financial Reform and Oil Spill Statutes. *Harvard Journal on Legislation* 48, 555–590.
Reidenberg JR (1997) Lex Informatica. The Formulation of Information Policy Rules through Technology. *Texas Law Review*, 76(3), 553–593.
Rothstein H, Huber M, Gaskell G (2006) A Theory of Risk Colonization: The Spiralling Regulatory Logics of Societal and Institutional Risk. *Economy and Society* 35(1), 91–112.
Rule J, McAdam D, Stearns L, Uglow D (1980) *The Politics of Privacy: Planning for Personal Data Systems as Powerful Technologies*. Elsevier, New York.
Schütz P (2012) The Set Up of Data Protection Authorities as a New Regulatory Approach. In: Gutwirth S, Leenes R, De Hert P, Poullet Y (eds) *European Data Protection – In Good Health?* pp. 125–142.Springer, Dordrecht.
Schwartz PM (1995) Privacy and Participation: Personal Information and Public Sector Regulation in the United States. *Iowa Law Review* 80, 553–618.
Simitis S (1984) Auf dem Weg zu einem neuen Datenschutzrecht. *Informatica e diritto* 3, 97–116.
Spinardi G (2019) Performance-Based Design, Expertise Asymmetry, and Professionalism: Fire Safety Regulation in the Neoliberal Era. *Regulation & Governance* 13, 520–539.
Taylor C (2020) GDPR at Risk of Failing Due to Underfunding of Regulators, Study Finds. *Irish Times* [Last accessed 27 April 2020.] Available from URL: https://www.irishtimes.com/business/technology/gdpr-at-risk-of-failing-due-to-underfunding-of-regulators-study-finds-1.4238927.
van Dijk N, Gellert R, Rommetveit K (2016) A Risk to a Right? Beyond Data Protection Risk Assessments. *Computer Law & Security Review* 32, 286–306.
Wright D, De Hert P (2012) *Privacy Impact Assessment*. Springer, Dordrecht.
Yeung K (2008) Towards an Understanding of Regulation by Design. In: Brownsword R, Yeung K (eds) *Regulating Technologies*, pp. 79–94.Hart Publishing, Portland, Oregon.
Yeung K (2015) Design for Regulation. In: Van den Hoven J, Van de Poel I, Vermaas PE (eds) *Handbook of Ethics, Values and Technological Design*, pp. 447–472.Springer, Dordrecht.
Zarsky T (2017) Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review* 47, 995–1020.

