Minds and Machines (2024) 34:13
https://doi.org/10.1007/s11023-024-09675-z

Regulation by Design: Features, Practices, Limitations, and Governance Implications

Kostina Prifti[1] · Jessica Morley[2] · Claudio Novelli[3] · Luciano Floridi[2,3]

Received: 13 February 2024 / Accepted: 22 April 2024 / Published online: 17 May 2024

Abstract

Regulation by design (RBD) is a growing research field that explores, develops, and criticises the regulative function of design. In this article, we provide a qualitative thematic synthesis of the existing literature. The aim is to explore and analyse RBD's core features, practices, limitations, and related governance implications. To fulfil this aim, we examine the extant literature on RBD in the context of digital technologies. We start by identifying and structuring the core features of RBD, namely the goals, regulators, regulatees, methods, and technologies. Building on that structure, we distinguish among three types of RBD practices: compliance by design, value creation by design, and optimisation by design. We then explore the challenges and limitations of RBD practices, which stem from risks associated with compliance by design, contextual limitations, or methodological uncertainty. Finally, we examine the governance implications of RBD and outline possible future directions of the research field and its practices.

Keywords Artificial intelligence · Design · Digital governance recommendations · Regulation by design · Technology regulation.

✉ Kostina Prifti
prifti@law.eur.nl

[1] Erasmus School of Law, Erasmus University Rotterdam, Burgemeester Oudlaan 50, Rotterdam 3062 PA, Netherlands

[2] Digital Ethics Center (DEC), Yale University, 85 Trumbull St, New Haven, CT 06511, USA

[3] Department of Legal Studies, University of Bologna, Via Zamboni, 27/29, Bologna 40126, Italy

1 Introduction

In recent years, the functional value of design has gained increasing relevance in regulatory governance theory, leading to what is generally referred to as 'Regulation By Design' (henceforth RBD).[1] The entry of design into these regulatory discussions follows a theoretical transition from a passive, *essentialist* view of regulation, which presents regulation as a set of rules enacted and enforced by the state (Baldwin et al., 1998; Hood, 1983), to an active, *functionalist* view, which presents regulation as having purposes beyond simply enforcing the law (e.g., modifying behaviour), thus expanding its scope to include additional mechanisms and actors (Black, 2001). Functional design has come to be viewed as a critical component of effective regulation because design can act as (a) another regulatory modality that provides constraints and affordances to regulatees, alongside law, markets, and community norms (Lessig, 1998, 1999); and (b) an enabler and facilitator of the regulative function of other regulatory modalities, such as the law (Reidenberg, 1997).

Murray and Scott have analysed the regulatory modalities that stem from the functionalist view in a framework comprising four *categories* of control – *hierarchical* (e.g., law), *community-based* (e.g., community norms), *competition-based* (e.g., markets), and *design-based* (e.g., code) – and three *forms* of control – standard setting, information gathering, and behaviour modification (Murray & Scott, 2002). These regulative modalities operate interrelatedly (Leenes & Lucivero, 2014). Design can be incorporated in the process of regulation by law, for instance, by outlining design-based requirements for organisations and designers, as well as after the implementation of regulation by law, for example, in developing a new technology product that modifies the behaviour of users by design.

RBD has become a widespread practice – for example, it informs the General Data Protection Regulation (GDPR) (Floridi, 2018) and the AI Act[2] – and a research field with increasing scholarly works. However, a critical analysis of this burgeoning literature, its core themes, and its influence on the development of the RBD concept is still missing. This is the gap we address in the following pages, by reviewing the literature on RBD in the context of digital technologies. We focus on digital technologies because of the inherent synergy between RBD literature and technological design.

The article is structured as follows. In section two, we elaborate on our methodological approach. In section three, we describe the core constituting features of RBD. In section four, we integrate and analyse these features to identify three types of RBD practices. In section five, we review the challenges and the limitations of these types of practices. In section six, we explore the future directions in the governance of RBD, as identified in various strands of scholarship. In section seven, we summarise our analysis and conclude the article by highlighting the study's limitations and suggesting areas for further research.

[1] Alternatively, it is also referred to as techno-regulation (Brownsword, 2016, 2019) or regulation by technology (Leenes, 2011).

[2] Art. 25 GDPR; Chap. 2 AI Act.

2 Methodology

Our literature review is based on the qualitative thematic synthesis methodology (Grant & Booth, 2009; Thomas & Harden, 2008). We begin by identifying the key features that define RBD. This involves an in-depth review of selected literature to pinpoint and list these features. In our case, the list includes: *goals*, *regulators*, *regulatees*, *methods*, and *technologies* of RBD. Next, we integrate, compare, and synthesise the individual analyses from qualitative studies in our sample, looking for intersectional features and constructing new themes. The first step has a descriptive function. The second step generates new interpretative constructs or explanations and focuses on the practices of RBD, the limitations of those practices, and related governance implications.

The question addressed is how to categorise and integrate the core conceptual and normative features, the practices, the limitations, and related governance implications of RBD. To answer this question, we select a sample of the literature from three databases, namely Scopus, Web of Science, and Google Scholar.[3] In Scopus and Web of Science, we used the following search criteria: '(regulation* "by design" OR governance* "by design" OR law* "by design") AND (technology* OR "artificial intelligence")' in title, keywords, and abstracts. In Google Scholar, we searched for 'regulation OR governance OR law "by design"' in the title, due to the differences in the search engines. As of December 2023, these criteria yielded 124 results in Web of Science, 435 in Scopus, and 218 in Google Scholar. We first excluded duplicates and inaccessible articles. Then, we scanned the titles and abstracts to assess and select the relevant articles for the review. Our main assessment criteria were language (only articles in English) and proximity to the relevant topic (only articles that referred to 'design' or 'by design' in the context of RBD). Consequently, our selected sample consisted of 174 articles. Some potentially relevant articles may not be included in our sample. A thematic synthesis review does not require an exhaustive collection of relevant articles but only a sample that is sufficiently representative to expect other relevant articles to fit with the results of our review work (Thomas & Harden, 2008, p. 3).

3 Regulation by Design: Goals, Regulators, Regulatees, Methods, and Technologies

Before presenting our review, two clarifications are in order. First, when discussing RBD, scholars address goals, regulators, regulatees, methods, and technology from two distinct perspectives: Governance, Ethical, Legal and Social Implications (GELSI) or Computer Science and Engineering (CS). These two approaches inform and influence each other, but as we shall see below, they also frequently diverge.

Second, RBD in the literature refers both to the forward-looking, constructionist role of design in the making of an artefact, which may be termed 'design *ad rem*', and

[3] We selected these databases for our review based on their comprehensive coverage, relevance to our research topic, and accessibility, ensuring a thorough exploration of existing scholarly works.

to the regulative effect of design in an environment, which can be intended or unintended and may be called 'design *in re*'. For example, designing smart grids to modernise and improve their efficiency, reliability, and sustainability (design *ad rem*) may have the intended effects of reducing carbon emissions and promoting clean energy (design *in re*). However, this design *ad rem* may have unintended design effects *in re*, resulting in harm to the privacy and security of personal data. In what follows, we shall use this terminology whenever it helps to avoid confusion.

3.1 The Purpose and Goals of Regulation by Design

According to the reviewed literature, the purpose of RBD concerns the regulative goal that design *ad rem* aims to fulfil. Despite a variety of 20 regulative goals advanced in the literature, the most common goal for RBD processes is privacy (89 papers), followed by data protection (28 papers).

This variety of goals in the literature reveals differences in levels of abstraction (Floridi, 2008). Some papers refer to high-level goals such as democracy, human rights, and the rule of law. Others refer to more granular, low-level goals such as contestability, explainability, and security (Table 1). The distinction between high- and low-level goals represents the granularity of analysis and the degree of practicality that we observe in the papers where those goals are discussed, with low-level goals linked to more practical and technical measures.

Given the distinct disciplinary backgrounds of GELSI and CS, it is no surprise that their approaches to the goals of RBD differ. GELSI scholars focus extensively on high-level goals, branching into two main viewpoints. The first promotes the advantages of design *ad rem*, while the second critiques the shortcomings of design *in re*. For instance, some research highlights the positive impact of focusing intentionally on the design of technologies, such as those deployed in smart cities, in achieving specific policy purposes like improving sustainability and participation in democratic processes (Helbing et al., 2021). Similar studies emphasise that the values of the rule of law, democracy, and human rights must be embedded in the design of technologies (Nemitz, 2018; Yeung et al., 2019). Conversely, a more critical stream of scholarship argues that the effects of rigid, compliance-oriented design solutions may often lead to reduced legal protection (Hildebrandt, 2015; Mulligan & Bamberger, 2018; Pagallo, 2012).

The CS literature typically focuses on low-level goals. Scholars have formulated methodologies for embedding privacy by design (Karim & Rawat, 2022; Thapa & Camtepe, 2021; Zalloum & Alamleh, 2020), for transparency by design (Schufrin et al., 2020), and for security by design (Tareke et al., 2018). Privacy by design often involves data protection and security because the solutions entail minimising data use (Conte et al., 2022) and making data more secure (Toli & Preneel, 2018), less accessible and less widely distributed (Zalloum & Alamleh, 2020).

In summary, although there is significant overlap between GELSI and CS scholarship, the GELSI literature focuses more extensively on high-level goals, for which they promote the need for design *ad rem* solutions without advancing detailed measures. When focusing on design *in re*, GELSI scholars adopt a critical approach to compliance-oriented solutions, underscoring their risks. CS scholarship, conversely,

Table 1 Levels of goals

Level	Goals	Example from the sample
Overarching	Regulation by design	Big data nudging operates as a type of regulation by design (Yeung, 2017)
High-level goals	Governance	Exploring the disruptive effects of governance by design concerning public governance and policymaking (Mulligan & Bamberger, 2018).
	Ethics	Developing tools that help designers reflect on the normative aspects of technologies (Urquhart & Rodden, 2016).
	Rule of law	The risks and limitations of embedding the rule of law in the design of technologies (Zalnieriute et al., 2020).
	Sustainability	Designing the digital realm in a distributed and participatory manner will lead to sustainability and democracy by design (Helbing et al., 2021).
	Human Rights	Human rights ought to be the normative framework for developing ethical AI (Yeung et al., 2019).
	Democracy	Experimental approaches, such as sandboxes, may help steer the design of technologies towards democratic values (Kera, 2020).
	Legal Protection	Legal protection must be integrated into the socio-technical infrastructure of ICT systems (Hildebrandt, 2015).
	Legality	Regulation by design must be used to steer designers and economic operators to comply with legal norms and principles (Van Cleynenbreugel, 2019)
	Autonomy	The regulative power of design should aim towards increasing the range of choices, instead of steering users towards compliance (Pagallo, 2012).
	Justice	Discussing which aspects of the design of smart grids are perceived to have justice implications by users (Milchram et al., 2020)
Low-level goals	Privacy	Privacy by design is an approach that helps companies develop a competitive advantage (Cavoukian, 2011).
	Data Protection	Analysing implementation challenges for data protection by design (Balboni et al., 2020).
	Safety	Analysing how safety by design is addressed in various engineering practices (van Gelder et al., 2021).
	Security	Assessing the utility of security by design for the development of information systems (Bygrave, 2022).
	Transparency	Ensuring that AI systems used in the public sector are transparent to citizens (Karkliniewska, 2022).
	Fairness	Analysing the legal, technical, and organisational limitations that hinder the aim of automating fairness (Wachter et al., 2021).
	Contestability	A contestability by design framework that enables data subjects to contest design choices at every stage of design and deployment before the contested decision (Almada, 2019).
	Explainability	Explainability of an AI system should focus on the design choices rather than on the technological system (Kroll, 2018)
	Loyalty	Ensuring that AI systems preserve and advance the interests of the users, in cases of a conflict of interest between the user and the organisation that has developed the AI system (Aguirre et al., 2021).

Table 2 Regulators of design

Regulators	Example
Designers	UX/UI designers may develop graphic design patterns that improve the information that users need to express valid consent (Dickhaut et al., 2021).
Policymakers	Public institutions must supervise, oversee, and verify the development of human rights-centred design (Nemitz, 2018; Yeung et al., 2019).
Both public and private actors	Impact assessments for safety by design require collaboration and deliberation from both public and private actors (Miettinen, 2021).
Organisations	The implementation of privacy by design requires internal support within the organisation (Levin, 2018).

Table 3 Regulatees of design

Regulatees	Example
Users (individual level)	'Legal by design' methods infringe on user's autonomy because they focus on ensuring strict compliance (Pagallo, 2016)
Technology	Designing a blockchain system where data is deleted automatically, following specific rule-based instructions (Farshid et al., 2019).
Society	The design of AI systems affects democracy, the rule of law, and human rights (Nemitz, 2018).
Organisations	The law must mandate rules that force organisations to implement PETs (Hornung, 2013).
Designers	Explainability obligations must focus on the designers rather than the technological system (Kroll, 2018).
Individual and Society	Technology should encourage people's change of behaviour by broadening their range of options, thus increasing both individual and collective autonomy (Pagallo, 2012).
All levels	The objectives of efficiency, accuracy, and utility, in the design of technologies, must be balanced with equitable treatment of different groups and the general public (Abiteboul & Stoyanovich, 2019).

tends to focus more on low-level goals, and advances operational solutions for design *ad rem*.

3.2 Regulators of Design

Regulators are *agents* that perform RBD (Table 2). Designers are the most frequently discussed regulators in the literature (103 papers). They occupy various roles within the practice of design. Designers may be system architects, UX/UI designers, front-/back-end developers, DevOps, testers, etc. CS papers are responsible for most of the attention on designers, as they explore how designers regulate the behaviour

of the technological system or the end user. The second most commonly examined regulators are policy-makers (36 papers), who use design and by-design solutions to advance public goals or supervise the implementation of legal by-design solutions (Nemitz, 2018; Yeung et al., 2019). Policymakers are more present in the GELSI literature. They occupy various roles that pursue a public interest, including legislators, civil servants, and non-governmental actors.

Other papers refer to structures that combine agents with a public interest and agents with a private interest, both acting as regulators. These papers usually focus on hybrid governance structures such as standardisation bodies (Kamara, 2017; Miettinen, 2021).

In addition, businesses and other economic operators (that is, organisations) have a role in RBD, even more so because of Article 25 of the GDPR, which obliges organisations, and not designers, to introduce technical solutions for data protection by design (Hildebrandt & Tielemans, 2013). The structures *within* organisations may support or inhibit the implementation of goals like privacy by design (Levin, 2018). Simultaneously, structures *between* organisations, such as market-based competition, may prove useful in incentivising the implementation of RBD goals within organisations (Grafenstein, 2019).

3.3 Regulatees of Design

Regulatees are *patients* (Floridi, 2013) who receive the effects of RBD (Table 3). Most contributions to the literature cast individual users as regulatees (73 papers). The GELSI literature focuses more on individual users, clarifying that design affects the choice set of users (Yeung, 2017), and the legal safeguards available to them (Hildebrandt, 2015). Often, technology itself is seen as an immediate regulatee (64 papers), since the design parameters essentially delineate the scope and limitations of a technological system's behaviour (Farshid et al., 2019). This view is at the fore of CS papers. Viewing technology as a regulatee implies that the immediate goal of RBD *ad rem* is to modify the behaviour of the technological system. In turn, such RBD *ad rem* affects users *in re*. Other types of regulatees refer to different levels of users, including society as a whole, both individuals and society, and all levels of users.

A separate set of contributions focuses on organisations and designers as receivers of legally mandated design obligations. In the case of organisations, the literature refers mostly to legal design obligations imposed on organisations about their role in the implementation of by-design solutions (Hornung, 2013; Tatar et al., 2020). Regarding designers, the literature discusses them as regulators by referring to legally mandated requirements that fall on them or how designers are affected by other existing designs and their regulative effects (Almada, 2019; Kroll, 2018).

3.4 Methods of Regulation by Design

Design performs its regulative function through various methods, which can be grouped into the following three categories: hardcoding requirements, softcoding requirements, and assessment criteria. First, hardcoding (Koops & Leenes, 2014)

entails designing rigid and inflexible rules that affect user behaviour and technological systems. Hardcoding requirements in the CS literature focus primarily on privacy and data protection goals. They aim at the *protection of information.* This approach manifests in technical solutions for data security, which can be centralised or decentralised. Such techniques are not intended to accommodate contextual variation, and their main strength is the possibility of (almost) automatic execution. Some examples of hardcoding from the reviewed sample include anonymisation (Campanile et al., 2021; Kühl et al., 2021; van Haaften et al., 2020), pseudonymisation (Conte et al., 2022; Kayem et al., 2021), data obfuscation and de-identification (Berg et al., 2021; Martinelli et al., 2020), and encryption (Karim & Rawat, 2022; Toli & Preneel, 2018; Vizitiu et al., 2019).

Second, softcoding (Tamo-Larrieux et al., 2021) is based on rules sensitive to the context, offering more autonomy and choice to the users (Koops & Leenes, 2014; Pagallo, 2016). Focusing primarily on privacy and data protection goals, softcoding methods aim at the *provision of information*, thus enabling users to have control over their privacy. The most common examples of softcoding include visual presentation interfaces that enhance user choice (Schufrin et al., 2020; Vasylkovskyi et al., 2021), consent-based frameworks (Agbo & Mahmoud, 2020; Khalid et al., 2023), and privacy self-management (Lobner et al., 2021).

Hardcoding and softcoding requirements are methods of design *ad rem* because they dictate how a system should be built for a specific goal. It is also possible to rely on assessment criteria, which form the third category of methods. Assessment criteria evaluate the risk and impact of a design on those who are or may be affected by it, known as regulatees. These threats may originate from the system's functioning or from contextual factors external to the system, such as the market structures on which the system is deployed. Some ancillary risks may also originate from the regulation itself, for instance, by imposing onerous obligations on developers, thereby discouraging innovation (Novelli et al., 2023b). Risk assessments are one example that features prominently in the literature on RBD (Bouchaut & Asveld, 2021). The other examples include data protection impact assessments (Miettinen, 2021; Papamartzivanos et al., 2021), and other types of impact assessments (Nemitz, 2018). Assessment criteria are used both in design *ad rem*, to evaluate the potential risks of the artefact during its design, and in design *in re*, to assess the impact of the artefact after it is made available for use.

Most of the literature focuses on requirements, with hardcoding (41 papers), softcoding (28 papers), or a combination of the two (32 papers) present in the majority of the papers that we reviewed. Only a minority of those papers examine the use of assessment criteria (22 papers). The remainder either discuss no specific RBD method or examine both requirements and assessment criteria (Table 4).

The GELSI and CS literature differ in their approach to the methods of RBD. CS papers focus mainly on requirements and minorly on assessment criteria. The opposite is true for GELSI papers, in which assessment criteria dominate. This stark contrast between the perspectives underscores the methodological challenges for interdisciplinary research and accentuates the need for a closer alignment between the perspectives.

Table 4 Methods of regulation by design

Methods of regulation by design	Example
Hardcoding	Developing an encryption method for privacy and security in biometric identification (Toli & Preneel, 2018).
Hardcoding and softcoding	Deploying privacy by design solutions for edge devices, combining both hardcoded and softcoded rules (Kunz et al., 2020)
Softcoding	Developing a mobile app that helps consumers compare standards and legal rules of different platforms (Noto La Diega, 2016)
Assessment and requirement criteria	A framework of assessment and requirement criteria for contestability by design that enables data subjects to contest not just the decision but the hypotheses and design choices at every stage of design and deployment before that decision (Almada, 2019).
Assessment criteria	Designing three levels of impact assessments for democracy, rule of law, and human rights by design (Nemitz, 2018)

3.5 The Technology of Regulation by Design

The literature on RBD treats the underlying technology either as a *target*, where it acts as a passive recipient of regulation, or as a *tool*, where it serves as a solution to achieve regulatory goals. The treatment of technology as a target includes cases when the technology is the immediate regulatee and when RBD focuses on the designers of that target technology.

The literature tends to refer to technology as a general target (37 papers), which entails an acontextual approach to RBD. This phenomenon is more present in GELSI papers. When the literature is more specific, it tends to focus on advanced forms of AI/robots, with a particular focus on healthcare applications. The most common types of target technologies are big data analysis (23 papers), healthcare AI/robots (14 papers), autonomous decision-making systems (ADM; 12 papers), and the Internet of Things (IoT; 11 papers). The literature reveals as many as 36 types of target technologies; however, in (Tables 5, 6), we list only the most cited types.

When technology is used as a solution for RBD goals, the most popular tools are blockchain (including smart contracts) and PETs (including encryption and anonymisation) (Table 7). Although there may be papers focusing on one specific tool of technological regulation (Hine et al., 2023), most highlight a range of different options (e.g., Guggenmos et al., 2020; Kühl et al., 2021; Posea et al., 2020). The GELSI and CS literature reveal essential differences in this case, too. GELSI papers either omit the discussion on the specific tool that is used for RBD, or they tend to focus on risk or impact assessments (Nemitz, 2018; Novelli et al., 2023a). Conversely, CS papers tend to be more explicit about the technology used for RBD, focusing primarily on blockchain and PETs.

Table 5 Technology as a target of regulation by design

Types of target technologies	Example
Technology	Design digital technologies so that the default setting for consent is negative (Grafenstein et al., 2021).
Big data analysis	Risk and impact assessments, in the context of big data analysis, enable organisations to consider by-design solutions, such as data minimisation (Mantelero, 2017)
Healthcare AI/robots	Developing and evaluating de-identification techniques for the re-use of unstructured clinical text (Berg et al., 2021)
AI (ADM)	Ensuring, through top-down rules, that ADMs used in the public sector are designed to be transparent (Karkliniewska, 2022)
IoT	Combining privacy by design, informed consent, and universal usability in IoT devices (O'Connor et al., 2017)
Blockchain	Designing a Privacy-Preserving Record Linkage protocol for blockchain technologies, which supports privacy by design (Nóbrega et al., 2021)
AI (broad)	Sustainability by design is a prerequisite for responsible, transparent, and human-centred AI (Perucica & Andjelkovic, 2022)
Online platforms	Developing a tool for transparency by design that helps users understand and analyse the data exported from online services (Schufrin et al., 2020)

4 Integrating the Features of Regulation by Design: A Typology of Practices

As the previous section revealed, the current literature highlights the multifaceted nature of RBD. Goals, regulators, regulatees, methods, and technologies differ widely. Table 7 contains a structured view of the features that comprise RBD as a phenomenon.

Such a structured view of the features of RBD can be instrumental in distinguishing different types of practices within the broad concept of RBD. These practices are formed not only by how they combine the various features of RBD, but especially by the perspective through which they approach the goal of RBD. In our review, we observed that the literature approaches the goals of RBD, whether high- or low-level, based on two distinct perspectives: compliance and value-based.

According to papers analysing the goals of RBD from the *compliance*-based perspective, a goal, much like a rule or a standard, entails a formal checklist of requirements. For example, the fulfilment of privacy is often equated with compliance with the GDPR rules for consent (Campanile et al., 2021; Metallidou et al., 2020). In

Table 6 Technology as a tool for regulation by design

Types of tools for regulation by design	Example
Blockchain	Relying on smart contracts to develop a consent management framework that provides patients with complete information over who and how their data are accessed (Agbo & Mahmoud, 2020)
PETs	Using various PETs for privacy and security in an IoT system (Malina et al., 2021)
Encryption	Developing encryption methods for privacy by design in healthcare AI that does not affect performance (Vizitiu et al., 2019)
Risk assessment	Adequate risk assessment and management for a safe-by-design approach requires regulatory flexibility, co-responsibility between researchers and stakeholders, and openness towards all stakeholders (Bouchaut & Asveld, 2021)
ML	Data security is pursued based on a decentralised federated learning model (Can & Ersoy, 2021)
IoT	Using IoT as a regulatory environment for the protection of privacy and interests of IoT users (Cheryl et al., 2021)

Table 7 The features of regulation by design

Features	Type	Example
Goal	High-level	Human Rights
	Low-level	Explainability
Method	Requirements (hardcoding)	Encryption
	Requirements (softcoding)	Consent-management
	Assessment	Risk assessment
Regulator	Designers	Modellers
	Policymakers	Legislative bodies
	Both public and private	Standardisation bodies
	Organisations	Data controllers
Regulatee	Users (various levels)	Data subjects
	Technology	Healthcare robots
	Organisations	Hospitals
	Designers	UX/UI designers
Technology	Target	Big data analysis
	Tool	PETs

contrast, according to papers analysing the goals of RBD from a *values*-based perspective, a goal entails any attempt to use design to increase a specific value within the regulatory system. To some extent, value-based approaches view goals as principles, which are norms to be realised proportionally, to the fullest extent possible (Alexy, 2000). For instance, when viewed as a value, advancing the goal of privacy may entail design choices that broaden the range of options for individuals (Pagallo, 2016). Not all the goals of RBD are subject to these two distinct perspectives; some are endemic to one. For instance, legality is a compliance-based goal, whereas legal

protection has a value-based background. Other goals, such as privacy, data protection, ethics, or fairness, are subject to treatment from both perspectives.

By integrating the structured view of the features of RBD with the types of perspectives on the goal of RBD, we can distinguish at least three types of RBD practices: compliance by design, value creation by design, and optimisation by design.

The first type, *compliance by design*, approaches any goal of RBD as a formal checklist of requirements. Consider, for example, design solutions prohibiting users from uploading illegal content on a platform. The application aims at legality as a goal, uses hardcoded requirements as methods, with designers as regulators, users as regulatees, the platform as a target, and machine learning as a tool that detects illegal content. Depending on the example, some of the features may change; compliance by design may also rely on softcoding requirements, such as nudging. However, the static features of compliance by design are users as regulatees and a compliance-oriented approach towards the goal of regulation.

The second type, *value creation by design*, is oriented towards design solutions that aim to increase that value in the regulatory system. An example can be using graphic design patterns that streamline information, making it more accessible and interactive for users to understand and use it. This application may have privacy as a goal, softcoding requirements as a method, designers as regulators, users as regulatees, cookie banners as targets, and graphic design patterns as tools. The application pursues privacy as a value by improving the provision of information that users may use for their privacy protection. The two static features of value creation by design are users as regulatees and a value-oriented approach towards the goal.

The third type, *optimisation by design*, is oriented towards compliance of the technological system with a particular standard, which is the goal of RBD. It is similar to compliance by design, except that the regulatee is the technological system, rather than the user. Consider anonymisation techniques. The pursued goal is privacy, utilising hardcoded requirements, with designers as regulators, technology as regulatee, applied to healthcare robots as a target, using anonymisation as a tool. This type of practice strives to optimise the behaviour of the technological system through a compliance-oriented approach. The two static features of optimisation by design are technology as a regulatee and a compliance-oriented approach towards the purpose of RBD.

Dissecting the types of practices through which RBD is applied helps us understand its criticisms more specifically. Instead of seeing these criticisms as objections to the whole concept, we can view them as objections to specific features or practices. For example, RBD has been criticised for being too rigid (Pagallo, 2021) and inflexible (Mantelero et al., 2020), for restricting user autonomy (Yeung, 2017), and for interfering with the rule of law (Hildebrandt, 2015; Brownsword, 2016). These criticisms proceed from the premise that RBD is directed at ensuring user compliance. As a result, they criticise a specific practice of RBD, namely compliance by design. This critique has led some scholars to call for designs that consider values, like fairness or privacy, instead of just enforcing rules efficiently (i.e., value-based and value-sensitive design) (Flanagan, 2018; Hildebrandt, 2011), which may be understood as a call for value creation by design.

If adopted, this typology introduces more nuance into current debates in the literature on RBD, such as the one that revolves around comparing compliance by design to value creation by design. In the following sections, we employ these distinctions to clarify RBD's diverse challenges and future directions.

5 The Challenges and Limitations of Regulation by Design

Thus far, we have examined the features and practices of RBD. However, many challenges and limitations undermine the potential of these practices for achieving regulatory purposes effectively. In this section, we will present a synthesised account of the challenges identified in the literature.

RBD faces three types of challenges. They stem from risks associated with compliance by design, contextual limitations, or methodological uncertainty.

Compliance by design poses several risks related to individual agency as an attempt to alter user behaviour, approaching the goal of regulation through compliance, and focusing on users as regulatees. This mode of RBD may reduce tolerance (Floridi, 2016), infringe on the autonomy of individuals (Pagallo, 2012), and violate the rule of law (Hildebrandt, 2015). Compliance by design can rely on hardcoded or softcoded rules. For instance, if policymakers wish to guarantee that drivers comply with the legal speed limit, they may use RBD in the shape of speedbumps (hardcoding) that force the driver to slow down. Alternatively, they may use nudging (softcoding) by equipping speed limit signs with digital displays that leverage social and emotional cues, i.e., when a driver obeys the speed limit, a smiley face is displayed, as opposed to a frown face displayed in the opposite case. The challenges that using hardcoded rules engenders appear graver because those rules are inflexible and acontextual (Lederman et al., 2016). In our example, speedbumps perform their regulative function on a reckless driver *and* an emergency vehicle (Floridi, 2016). However, softcoding techniques can also considerably impact individuals' autonomy (Schmidt & Engelen, 2020). On the whole, compliance by design is liable to systemic harm (Zalnieriute et al., 2020), particularly because public actors, including the courts, may lack the expertise to exercise their typical supervisory functions in this domain (Mulligan & Bamberger, 2018).

A second challenge relates to contextual limitations, which manifest in one version of value creation by design. That version prioritises providing meaningful information to empower individuals to exercise their rights and self-determination. This orientation is reflected in frameworks like pro-ethical design (Floridi, 2016), privacy self-management (Agbo & Mahmoud, 2020), or consent management (Calani et al., 2021), which aim to enhance the quality and the quantity of the information that is provided to users. Such reliance on information provision sets unrealistic expectations in contexts where (a) frequent expressions of consent are needed or (b) information complexity is high. Cookie banners, known to induce consent fatigue, are a salient example of settings where information provision fails to deliver on its objectives (Choi et al., 2018). The problem of complex information is exemplified by ADMs (Prifti et al., 2023). Individuals may lack knowledge of the intended use of information or fail to grasp it. Even if they are informed and knowledgeable, they

may not possess the resources, e.g., time and money, necessary to use the information to their advantage (Yeung, 2017). These problems are exacerbated by the various power imbalances in the relationship between organisations and individuals. Organisations generally seek to extract information. Individuals, conversely, are assumed to be interested in protecting their rights and ensuring that organisations comply with the law. These expectations are often based on the information provided to individuals by those same organisations (Rommetveit et al., 2017; Finn & Wadhwa, 2014). Such a burden imposed on individuals results in misalignments between design *ad rem*, where the system is intentionally built so that information provision and user controls enhance legal protection, and design *in re*, where contextual factors like information overload, ignorance about how the provided information can be used, and resource scarcity compromise the effectiveness of legal protection.

The third challenge for RBD is the methodological and epistemological problem of operationalising open-ended normative concepts (e.g., ethical principles) into workable solutions for design *ad rem*. Translating values into engineering solutions is not straightforward (Koops & Leenes, 2014; Tamo-Larrieux et al., 2021). Designers enjoy a margin of discretion in redefining the concepts through implicit and explicit decisions (Rommetveit et al., 2017; Rommetveit & van Dijk, 2022). For example, we may consider the design of digital twins, which are virtual representations of a physical system that help improve decision-making over that system by testing different scenarios without affecting the physical system. Digital twins are used, among other contexts, for wind turbines' safety, reliability, and optimal efficiency (Solman et al., 2022). While designing digital twins, designers must translate the themes of the physical system into the virtual representation. However, some themes may be represented inadequately or incompletely. In the case of designing digital twins of wind turbines, landscape considerations were reduced to a single theme of 'visual impact'. As a result, these methodological choices impacted the decision-making for wind turbine governance, since the governance decisions were based on the visual representation embodied in digital twins (Solman et al., 2022).

This methodological challenge generates legitimacy concerns on the input, throughput, and output levels (Schmidt, 2013). Input legitimacy pertains to the inclusiveness and representativeness of the stakeholders involved in the decision-making process. Concerns arise when users and other affected groups are not adequately involved or represented during critical stages of the design processes where methodological choices are made. Throughput legitimacy concerns the transparency and accountability of the design processes, that is, when decision-making is not transparent or when those responsible for the choices are not held accountable. Output legitimacy concerns the effects and effectiveness of the RBD. Problems occur when the methodological choices made during the design *ad rem* stage have an unjust or undesirable effect on users *in re*.

6 Digital Governance: Future Directions in Regulation by Design

The three challenges and limitations highlighted in the preceding section hinder the potential and may compromise the intended effects of RBD. Fortunately, they can be overcome, or at least mitigated, through Digital Governance, which is the practice of implementing policies, procedures, and standards for the proper development and management of the infosphere (Floridi, 2018). Digital Governance, thus, may account for the regulative function of design and steer the practices of RBD.

Depending on the nature of the actors, governance can be private, public, or hybrid. RBD may be embedded in private governance structures through self-regulatory measures. The literature has explored how organisations can effectively integrate by-design solutions into their structures (Picker, 2011). Two recurring themes are the need for senior managers to support privacy assimilation processes (Attili et al., 2022) and for general internal support, which need not take the form of establishing a privacy office (Levin, 2018). Despite their limited function, market-based, self-regulatory mechanisms are insufficient, necessitating public governance involvement (Bygrave, 2022; Hornung, 2013; Nemitz, 2018).

Public governance solutions, such as legislation and administrative policies, can oblige and guide designers and organisations to implement by-design solutions (Hildebrandt & Tielemans, 2013; Hornung, 2013). Public agencies should enforce the resultant legal requirements (Nemitz, 2018; Yeung et al., 2019). Based on the reviewed literature, we suggest considering two approaches: extending the supervisory functions of public bodies and enabling participation. First, public bodies must evaluate the extent to which legal and ethical principles are reflected in the design of technological systems (Yeung et al., 2019). This form of oversight may help mitigate the risks arising from compliance by design and the limitations of information-provision frameworks identified on the preceding pages. Oversight competencies are usually allocated to data protection authorities (DPAs), which need not be the case (Brown, 2014). It may be desirable to rely on other public actors, such as the courts (Bygrave, 2022; Vivarelli, 2020). Additionally, broader public oversight may take the form of third-party auditing, which may further facilitate the oversight by public institutions (Raji et al., 2022). Second, the participation of users and interested stakeholders from the broader public may support the goals of public governance (Helbing et al., 2021; Lederman et al., 2016; Miettinen, 2021). The literature has underscored the importance of collaboration with different stakeholders when making design decisions (Bouchaut & Asveld, 2020, 2021; Brown, 2014). Specifically, regulatory sandboxes can enhance stakeholder participation by allowing the affected and interested groups to provide input into the design of technologies (De Filippi et al., 2022; Kera, 2020).

Hybrid governance, characterised by the involvement of public and private actors, is also relevant for RBD practices (Van Cleynenbreugel, 2019). The EU prefers hybrid governance for its product safety regulation; requirements are outlined in EU law and then specified during European standardisation (Weatherill, 2013), a strategy also employed in formulating the AI Act (2021). The principal advantages of hybrid governance are linked to broader expertise and enhanced flexibility (Joerges et al., 1999), which are useful in technical and highly dynamic domains such as RBD.

Furthermore, hybrid governance can incentivise organisations to innovate and gain a competitive advantage (Gottardo et al., 2021; Grafenstein, 2019). However, the legitimacy of hybrid governance is often questionable. Private actors use their expertise in standardisation to advance their private interests (Kamara, 2017; Mulligan & Bamberger, 2018; Van Cleynenbreugel, 2019), which can undermine the normative requirements of public governance (Almada, 2023; Veale & Borgesius, 2021). Furthermore, the technical know-how that RBD requires is still being accumulated, and best practices are yet to crystallise (Burkart & Huber, 2021). Consequently, there is an epistemic gap between the objectives of governance and the technical state of the art, which may lead to regulatory uncertainty.

Regulatory uncertainty requires more interdisciplinary work, both in research and policymaking. Specifically, we believe a closer alignment between GELSI and CS scholarships is needed. In the current landscape, while authors from these two fields do refer to each other's work, their analyses are not sufficiently integrated. For instance, GELSI scholars highlight the practical and contextual limitations of information-provision frameworks; however, the implications of their findings have not been fully internalised in the CS literature. Closer alignment between GELSI and CS studies should enable a shift from compliance and optimisation by design, which are paradigmatic in the CS literature, to value creation by design, which is more prominent in GELSI scholarship. Likewise, the GELSI literature should reflect the technical reality that the CS literature describes. Firmer grounding in design *ad rem* and a more acute awareness of technical developments are needed in governance. Such an alignment between the two perspectives may contribute to evidence-based policymaking by formulating experimental methods that require cooperation between policymakers, technical experts, and stakeholders (Sucha & Sienkiewicz, 2020).

7 Conclusions

In this article, we provided a qualitative thematic synthesis of RBD as advanced and developed in the extant literature. We focused on its conceptual, normative, and applied elements. We first developed a structured view of the many features characterising RBD, which enables more granular analyses of the concept and more nuanced distinctions between its different applications and related criticisms. We then reviewed and highlighted the challenges that regulators and policymakers must approach carefully and precisely, before exploring digital governance implications and future directions of RBD.

The scope of our study limits the results of this article. We have reviewed only works in the English language published no later than 2023 and have conducted the literature review of RBD based on search terms that contained combinations of 'by design' with 'regulation', 'governance', or 'law', in the context of digital technologies. As a result, some contributions may not have been captured by the search design choices and may have been overlooked, such as those focusing on RBD without a clear reference to the research field. Further research may offset these limitations by expanding the search terms and scope of the review.

The analysis and results presented in this article aim to enable further, more granular analyses of RBD. First, we aim to guide further research that focuses on specific practices of RBD, whether that research advances a new solution or criticises existing practices. Second, by exposing the methodological gap between GELSI and CS scholarship in their treatment of RBD, we hope to initiate a closer alignment and more interdisciplinarity between these two perspectives. Such alignment is valuable to both perspectives, considering that, as discussed in the preceding pages, the risks and challenges associated with RBD span multiple disciplines, necessitating interdisciplinary approaches and solutions. Third, by exploring and categorising the available technical solutions, we hope to guide policymakers to account for and steer the practices of RBD. In this regard, we believe that more space is required for the role of public institutions in overseeing and steering the practice of RBD. For example, public institutions may guide and support the alignment between GELSI and CS scholarships by allocating research funds for projects that combine scholars from the two perspectives. They may also steer the practices of RBD by mandating or incentivising particular design solutions that better support public goals. Finally, assuming these three recommended developments materialise, we anticipate RBD solutions to transition from compliance and optimisation by design towards value creation by design. Compliance and optimisation are requirements, often mandated by law, but pursuing value creation by design enables private regulators to go beyond the legal requirements and fully harness the regulative potential of design in a value-oriented way.

Acknowledgements Prifti's work is part of the research initiative on 'Rebalancing of Public Interests in Private Relationships', the sector plan for law funding of the Dutch Ministry of Education, Culture and Research. This research has been made possible also thanks to the financial support of Banca Intesa Sanpaolo, through the University of Bologna.

Declarations

Conflict of interest Authors declare no conflict of interest.

References

Abiteboul, S., & Stoyanovich, J. (2019). Transparency, fairness, data protection, neutrality: Data management challenges in the face of new regulation. *Journal of Data and Information Quality*, *11*(3). https://doi.org/10.1145/3310231.

Agbo, C. C., & Mahmoud, Q. H. (2020). Design and Implementation of a Blockchain-Based E-Health Consent Management Framework. *Conference Proceedings - IEEE International Conference on Systems, Man and Cybernetics*, *2020-October*, 812–817.https://doi.org/10.1109/SMC42975.2020.9283203.

Aguirre, A., Reiner, P. B., Surden, H., & Dempsey, G. (2021). *AI Loyalty by Design: A Framework for Governance of AI*.

Alexy, R. (2000). On the structure of Legal principles. *Ratio Juris*, *13*(3), 294–304. https://doi.org/10.1111/1467-9337.00157.

Almada, M. (2019). Human intervention in automated decision-making: Toward the construction of contestable systems. *Proceedings of the 17th International Conference on Artificial Intelligence and Law ICAIL 2019*, *2-11*. https://doi.org/10.1145/3322640.3326699.

Almada, M. (2023). Regulation by design and the governance of Technological futures. *European Journal of Risk Regulation*, *14*(4), 697–709. https://doi.org/10.1017/err.2023.37.

Attili, V. S. P., Mathew, S. K., & Sugumaran, V. (2022). Information privacy assimilation in IT Organizations. *Information Systems Frontiers*, *24*(5), 1497–1513. https://doi.org/10.1007/s10796-021-10158-0.

Balboni, P., Francis, K., Botsi, A., & Barata, M. T. (2020). Designing connected and automated vehicles around legal and ethical concerns: Data protection as a corporate social responsibility. *CEUR Workshop Proceedings*, *2844*, 139–151. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85104660519&partnerID=40&md5=51f78bdd7823ccd57f251e2cbc40ecef.

Baldwin, R., Scott, C., Hood, C., Baldwin, R., Scott, C., & Hood, C. (Eds.). (1998). *A reader on Regulation*. Oxford University Press.

Berg, H., Henriksson, A., Fors, U., & Dalianis, H. (2021). De-identification of clinical text for secondary use: Research issues. *HEALTHINF 2021–14th International Conference on Health Informatics; Part of the 14th International Joint Conference on Biomedical Engineering Systems and Technologies, BIOSTEC 2021*, 592–599.https://www.scopus.com/inward/record.uri?eid=2-s2.0-85103860417&partnerID=40&md5=c5a05373cd0e4c805d402f5b01b36ad5

Black, J. (2001). Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. *Current Legal Problems*, *54*. https://doi.org/10.1093/clp/54.1.103.

Bouchaut, B., & Asveld, L. (2020). Safe-by-Design: Stakeholders' perceptions and expectations of how to Deal with Uncertain risks of emerging Biotechnologies in the Netherlands. *RISK ANALYSIS*, *40*(8), 1632–1644. https://doi.org/10.1111/risa.13501.

Bouchaut, B., & Asveld, L. (2021). Responsible learning about risks arising from emerging Biotechnologies. *Science and Engineering Ethics*, *27*(2). https://doi.org/10.1007/s11948-021-00300-1. .

Brown, I. (2014). Britain's smart meter programme: A case study in privacy by design. *International Review of Law Computers and Technology*, *28*(2), 172–184. https://doi.org/10.1080/13600869.2013.801580.

Brownsword, R. (2016). Technological management and the rule of Law. *Law Innovation and Technology*, *8*(1), 100–140. https://doi.org/10.1080/17579961.2016.1161891.

Brownsword, R. (2019). *Law, Technology and Society: Reimagining the Regulatory Environment*. Routledge & CRC. https://www.routledge.com/Law-Technology-and-Society-Reimagining-the-Regulatory-Environment/Brownsword/p/book/9780815356462.

Burkart, N., & Huber, M. F. (2021). A survey on the explainability of supervised machine learning. *Journal of Artificial Intelligence Research*, *70*, 245–317.

Bygrave, L. A. (2022). Security by design: Aspirations and realities in a Regulatory Context. *Oslo Law Review*, *8*(3), 126–177. https://doi.org/10.18261/olr.8.3.2.

Calani, M., Denaro, G., & Leporati, A. (2021). Exploiting the blockchain to guarantee GDPR compliance while consents evolve under data owners' control. *CEUR Workshop Proceedings*, *2940*, 331–343. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114927715&partnerID=40&md5=23214413d66ff9431a69dd41baec78b3

Campanile, L., Iacono, M., Marulli, F., & Mastroianni, M. (2021). Designing a GDPR compliant blockchain-based IoV distributed information tracking system. *Information Processing and Management*, *58*(3). https://doi.org/10.1016/j.ipm.2021.102511.

Can, Y. S., & Ersoy, C. (2021). Privacy-preserving Federated Deep Learning for Wearable IoT-based Biomedical Monitoring. *ACM Transactions on Internet Technology*, *21*(1). https://doi.org/10.1145/3428152.

Cavoukian, A. (2011). *Privacy by design in law, policy and practice: A white paper for regulators, decision-makers and policy-makers*. Information and Privacy Commissioner of Ontario.

Cheryl, B., Ng, B., & Wong, C. (2021). Governing the progress of internet-of-things: Ambivalence in the quest of technology exploitation and user rights protection. *TECHNOLOGY IN SOCIETY*, 64. https://doi.org/10.1016/j.techsoc.2020.101463.

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, *81*, 42–51. https://doi.org/10.1016/j.chb.2017.12.001.

Conte, R., Sansone, F., Tonacci, A., & Pala, A. P. (2022). Privacy-by-design and minimization within a small Electronic Health Record: The Health360 case study. *Applied Sciences (Switzerland)*, *12*(17). https://doi.org/10.3390/app12178441.

De Filippi, P., Mannan, M., & Reijers, W. (2022). The alegality of blockchain technology. *Policy and Society*, *41*(3), 358–372. https://doi.org/10.1093/polsoc/puac006.

Dickhaut, E., Li, M. M., Janson, A., & Leimeister, J. M. (2021). Developing lawful technologies—A revelatory case study on design patterns. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-January*, 4384–4393. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85103348242&partnerID=40&md5=5f98d8b44421338cfe8e3b3c0bf426a7

Farshid, S., Reitz, A., & Roßbach, P. (2019). Design of a forgetting blockchain: A possible way to accomplish GDPR compatibility. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2019-January*, 7087–7095. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85081554455&partnerID=40&md5=1fa8891bd4035a2708721f9d41d10aa9

Finn, R.L., & K. Wadhwa. (2014). The ethics of "Smart" advertising and regulatory initiatives in the consumer intelligence industry. Info 16, no. 3: 22–39. https://doi.org/10.1108/info-12-2013-0059

Flanagan, R. (2018). Better by design: Implementing Meaningful Change for the Next Generation of Law students. *Me L Rev*, *71*, 103.

Floridi, L. (2008). The method of levels of abstraction. *Minds and Machines*, *18*(3), 303–329. https://doi.org/10.1007/s11023-008-9113-7.

Floridi, L. (2013). *The Ethics of Information*. Oxford University Press.

Floridi, L. (2016). Tolerant Paternalism: Pro-ethical Design as a resolution of the Dilemma of Toleration. *Science and Engineering Ethics*, *22*(6), 1669–1688. https://doi.org/10.1007/s11948-015-9733-2.

Floridi, L. (2018). Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of the Royal Society A: Mathematical Physical and Engineering Sciences*, *376*(2133), 20180081. https://doi.org/10.1098/rsta.2018.0081.

Gottardo, S., Mech, A., Drbohlavová, J., Małyska, A., Bøwadt, S., Riego Sintes, J., & Rauscher, H. (2021). Towards safe and sustainable innovation in nanotechnology: State-of-play for smart nanomaterials. *NanoImpact*, *21*https://doi.org/10.1016/j.impact.2021.100297.

Grafenstein, M. (2019). Co-Regulation and the Competitive Advantage in the GDPR: Data Protection Certification Mechanisms, Codes of Conduct and the'State of the Art'of Data Protection-by-Design. *Forthcoming in González-Fuster, G., van Brakel, R. and P. De Hert Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics, Edward Elgar Publishing*.

Grafenstein, M., Heumüller, J., Belgacem, E., Jakobi, T., & Smiesko, P. (2021). Effective Regulation through Design–Aligning the ePrivacy Regulation with the EU General Data Protection Regulation (GDPR): Tracking Technologies in Personalised Internet Content and the Data Protection by Design Approach. *Available at SSRN 3945471*.

Grant, M. J., & Booth, A. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, *26*(2), 91–108. https://doi.org/10.1111/j.1471-1842.2009.00848.x.

Guggenmos, F., Rieger, A., Wenninger, A., Fridgen, G., & Lockl, J. (2020). How to develop a GDPR-compliant blockchain solution for cross-organizational workflow management: Evidence from the German asylum procedure. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-January*, 4023–4032. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85099255047&partnerID=40&md5=0899a8dfe4f71d3e98e9b8ceb9ce18bd

Helbing, D., Fanitabasi, F., Giannotti, F., Hanggli, R., Hausladen, C., van den Hoven, J., Mahajan, S., Pedreschi, D., & Pournaras, E. (2021). Ethics of Smart cities: Towards Value-Sensitive Design and Co-evolving City Life. *Sustainability*, *13*(20). https://doi.org/10.3390/su132011162.

Hildebrandt, M. (2011). Legal Protection by Design: Objections and refutations. *Legisprudence*, *5*(2), 223–248. https://doi.org/10.5235/175214611797885693.

Hildebrandt, M. (2015). The public(s) on life: A call for legal protection by design. In *The Onlife Manifesto: Being Human in a Hyperconnected Era* (pp. 181–193). https://doi.org/10.1007/978-3-319-04093-6_19.

Hildebrandt, M., & Tielemans, L. (2013). Data protection by design and technology neutral law. *Computer Law and Security Review*, *29*(5), 509–521. https://doi.org/10.1016/j.clsr.2013.07.004.

Hine, E., Novelli, C., Taddeo, M., & Floridi, L. (2023). Supporting trustworthy AI through machine unlearning. *SSRN Scholarly Paper 4643518*. https://doi.org/10.2139/ssrn.4643518.

Hood, C. (1983). *The tools of government*. Macmillan.

Hornung, G. (2013). Regulating privacy enhancing technologies: Seizing the opportunity of the future European Data Protection Framework. *Innovation: The European Journal of Social Science Research*, *26*(1–2), 181–196. https://doi.org/10.1080/13511610.2013.723381.

Joerges, C., Schepel, H., & Vos, E. (1999). *The Law's Problems with the Involvement of Non-Governmental Actors in Europe's Legislative Processes: The Case of Standardisation under the 'New Approach'*.

Kamara, I. (2017). Co-regulation in EU personal data protection: The case of technical standards and the privacy by design standardisation'mandate'. *European Journal of Law and Technology*, *8*(1).

Karim, H., & Rawat, D. B. (2022). TollsOnly please—homomorphic encryption for toll transponder privacy in Internet of vehicles. *IEEE Internet of Things Journal*, *9*(4), 2627–2636. https://doi.org/10.1109/JIOT.2021.3056240.

Karkliniewska, I. (2022). Building transparency and robustness of AI/ADM Management in Public Sector. *CEUR Workshop Proceedings*, *3285*, 1–7. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85143392706&partnerID=40&md5=048487d6b502d07e81cc8a590341b46d

Kayem, A. V. D. M., Podlesny, N. J., Meinel, C., & Lehmann, A. (2021). On chameleon pseudonymisation and attribute compartmentation-as-a-service. *Proceedings of the 18th International Conference on Security and Cryptography, Secrypt 2021*, 704–714. https://doi.org/10.5220/0010552207040714.

Kera, D. R. (2020). *Experimental Algorithmic Citizenship in the Sandboxes: An Alternative to Ethical Frameworks and Governance-by-Design Interventions*.

Khalid, M. I., Ahmed, M., Helfert, M., & Kim, J. (2023). Privacy-First Paradigm for Dynamic Consent Management Systems: Empowering Data Subjects through Decentralized Data Controllers and Privacy-Preserving Techniques. *Electronics*, 12(24), Article 24. https://doi.org/10.3390/electronics12244973.

Koops, B. J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design'provision in data-protection law. *International Review of Law Computers & Technology*, *28*(2), 159–171.

Kroll, J. (2018). The fallacy of inscrutability. *Philosophical Transactions of the Royal Society A-Mathematical Physical and Engineering Sciences*, *376*(2133). https://doi.org/10.1098/rsta.2018.0084.

Kühl, N., Martin, D., Wolff, C., & Volkamer, M. (2021). Healthy surveillance: Designing a concept for privacy-preserving mask recognition AI in the age of pandemics. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-January*, 1706–1715. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85108333137&partnerID=40&md5=402f1fd726df63b7426b72798b726e1b

Kunz, I., Stephanow, P., & Banse, C. (2020). An Edge Framework for the Application of Privacy Enhancing Technologies in IoT Communications. *IEEE International Conference on Communications*, *2020-June*. https://doi.org/10.1109/ICC40277.2020.9149344.

La Noto, G. (2016). *Uber law and awareness by design. An empirical study on online platforms and dehumanised negotiations*.

Lederman, J., Taylor, B. D., & Garrett, M. (2016). A private matter: The implications of privacy regulations for intelligent transportation systems. *Transportation Planning and Technology*, *39*(2), 115–135. https://doi.org/10.1080/03081060.2015.1127537.

Leenes, R. (2011). Framing Techno-Regulation: An Exploration of State and Non-state Regulation by Technology. *Legisprudence*, *5*(2), 143–169. https://doi.org/10.5235/175214611797885675.

Leenes, R., & Lucivero, F. (2014). Laws on Robots, laws by Robots, laws in Robots: Regulating Robot Behaviour by Design. *Law Innovation and Technology*, *6*(2), 193–220. https://doi.org/10.5235/17579961.6.2.193.

Lessig, L. (1998). The New Chicago School. *The Journal of Legal Studies*, *27*(S2), 661–691. https://doi.org/10.1086/468039.

Lessig, L. (1999). *Code and other laws of Cyberspace*. Basic Books, Inc.

Levin, A. (2018). Privacy by design by regulation: The Case Study of Ontario. *Can J Comp & Contemp L*, *4*, 115.

Lobner, S., Tesfay, W. B., Nakamura, T., & Pape, S. (2021). Explainable machine learning for default privacy setting prediction. *Ieee Access : Practical Innovations, Open Solutions*, *9*, 63700–63717. https://doi.org/10.1109/ACCESS.2021.3074676.

Malina, L., Dzurenda, P., Ricci, S., Hajny, J., Srivastava, G., Matulevicius, R., Affia, A. A. O., Laurent, M., Sultan, N. H., & Tang, Q. (2021). Post-quantum era privacy protection for intelligent infrastructures. *Ieee Access : Practical Innovations, Open Solutions*, *9*, 36038–36077. https://doi.org/10.1109/ACCESS.2021.3062201.

Mantelero, A. (2017). Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer Law and Security Review*, *33*(5), 584–602. https://doi.org/10.1016/j.clsr.2017.05.011.

Mantelero, A., Vaciago, G., Samantha Esposito, M., & Monte, N. (2020). The common EU approach to personal data and cybersecurity regulation. *International Journal of Law and Information Technology*, *28*(4), 297–328. https://doi.org/10.1093/ijlit/eaaa021.

Martinelli, F., Marulli, F., Mercaldo, F., Marrone, S., & Santone, A. (2020). Enhanced privacy and Data Protection using Natural Language Processing and Artificial Intelligence. *Proceedings of the International Joint Conference on Neural Networks*, *Scopus*. https://doi.org/10.1109/IJCNN48605.2020.9206801.

Metallidou, C., Psannis, K. E., & Alexandropoulou-Egyptiadou, E. (2020). An efficient IoT System respecting the GDPR. *2020 3rd World Symposium on Communication Engineering WSCE 2020*, *79-83*https://doi.org/10.1109/WSCE51339.2020.9275573.

Miettinen, M. (2021). By design and risk regulation: Insights from nanotechnologies. *European Journal of Risk Regulation*, *12*(4), 775–791.

Milchram, C., Künneke, R., Doorn, N., van de Kaa, G., & Hillerbrand, R. (2020). Designing for justice in electricity systems: A comparison of smart grid experiments in the Netherlands. *Energy Policy*, *147*https://doi.org/10.1016/j.enpol.2020.111720.

Mulligan, D., & Bamberger, K. (2018). Saving Governance-By-Design. *California Law Review*, *106*(3), 697–784. https://doi.org/10.15779/Z38QN5ZB5H.

Murray, A., & Scott, C. (2002). Controlling the New Media: Hybrid responses to New forms of Power. *The Modern Law Review*, *65*(4), 491–516. https://doi.org/10.1111/1468-2230.00392.

Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society A-Mathematical Physical and Engineering Sciences*, *376*(2133). https://doi.org/10.1098/rsta.2018.0089.

Nóbrega, T., Pires, C. E. S., & Nascimento, D. C. (2021). Blockchain-based Privacy-Preserving Record Linkage: Enhancing data privacy in an untrusted environment. *Information Systems*, *102*. https://doi.org/10.1016/j.is.2021.101826.

Novelli, C., Casolari, F., Rotolo, A., Taddeo, M., & Floridi, L. (2023a). *How to Evaluate the Risks of Artificial Intelligence: A Proportionality-Based, Risk Model for the AI Act* (SSRN Scholarly Paper 4464783). https://doi.org/10.2139/ssrn.4464783.

Novelli, C., Casolari, F., Rotolo, A., Taddeo, M., & Floridi, L. (2023b). Taking AI risks seriously: A new assessment model for the AI act. *AI & SOCIETY*. https://doi.org/10.1007/s00146-023-01723-z.

O'Connor, Y., Rowan, W., Lynch, L., & Heavin, C. (2017). Privacy by design: Informed consent and internet of things for Smart Health. *Procedia Computer Science*, *113*, 653–658. https://doi.org/10.1016/j.procs.2017.08.329.

Pagallo, U. (2012). Cracking down on autonomy: Three challenges to design in IT Law. *Ethics and Information Technology*, *14*(4), 319–328. https://doi.org/10.1007/s10676-012-9295-9.

Pagallo, U. (2016). The impact of domestic robots on privacy and data protection, and the troubles with legal regulation by design. *Data protection on the move* (pp. 387–410). Springer.

Pagallo, U. (2021). On the principle of privacy by design and its limits: Technology, ethics and the rule of law. *Italian philosophy of Technology* (pp. 111–127). Springer.

Papamartzivanos, D., Menesidou, S. A., Gouvas, P., & Giannetsos, T. (2021). A perfect match: Converging and automating privacy and security impact assessment on-the-fly. *Future Internet*, *13*(2), 1–34. https://doi.org/10.3390/fi13020030.

Perucica, N., & Andjelkovic, K. (2022). Is the future of AI sustainable? A case study of the European Union. *Transforming Government: People Process and Policy*, *16*(3), 347–358. https://doi.org/10.1108/TG-06-2021-0106.

Picker, R. C. (2011). Unjustified by Design: Unfairness and the FTC's Regulation of Privacy and Data Security. *Draft), Law and Economics Center, George Mason University, Online Copy Dated May*, *13*.

Posea, V., Nitu, C., Damian, C., Panu, A., & Alboaie, L. (2020). GDPR Compliant Recruitment Platform using Smart Contracts and Executable Choreographies. *EPE 2020 - Proceedings of the 2020 11th International Conference and Exposition on Electrical And Power Engineering*, 103–108. https://doi.org/10.1109/EPE50722.2020.9305669.

Prifti, K., Krijger, J., Thuis, T., & Stamhuis, E. (2023). From bilateral to Ecosystemic transparency: Aligning GDPR's transparency obligations with the European Digital Ecosystem of Trust. In S. Kuhlmann, De F. Gregorio, M. Fertmann, H. Ofterdinger, & A. Sefkow (Eds.), *Transparency or opacity* (pp. 115–140). Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748936060-115.

Raji, I. D., Xu, P., Honigsberg, C., & Ho, D. (2022). Outsider Oversight: Designing a Third Party Audit Ecosystem for AI Governance. *Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society*, 557–571. https://doi.org/10.1145/3514094.3534181.

Reidenberg, J. R. (1997). Lex Informatica: The Formulation of Information Policy rules through Technology. *Texas Law Review*, *76*(3), 553–594.

Rommetveit, K., & van Dijk, N. (2022). Privacy engineering and the techno-regulatory imaginary. *Social Studies of Science*, *52*(6), 853–877. https://doi.org/10.1177/03063127221119424.

Rommetveit, K., Tanas, A., & van Dijk, N. (2017). *Data protection by design: Promises and perils in crossing the Rubicon between law and engineering*. 25–37.

Schmidt, V. A. (2013). Democracy and legitimacy in the European Union Revisited: Input, output and 'Throughput'. *Political Studies*, *61*(1), 2–22. https://doi.org/10.1111/j.1467-9248.2012.00962.x.

Schmidt, A. T., & Engelen, B. (2020). The ethics of nudging: An overview. *Philosophy Compass*, *15*(4), e12658. https://doi.org/10.1111/phc3.12658.

Schufrin, M., Reynolds, S. L., Kuijper, A., Kohlhammer, J., & the Internet. (2020). A Visualization Interface to Improve the Transparency of Collected Personal Data on. *2020 IEEE Symposium on Visualization for Cyber Security, VizSec 2020*, 1–10. https://doi.org/10.1109/VizSec51108.2020.00007.

Solman, H., Kirkegaard, J. K., Smits, M., Van Vliet, B., & Bush, S. (2022). Digital twinning as an act of governance in the wind energy sector. *Environmental Science and Policy*, *127*, 272–279. https://doi.org/10.1016/j.envsci.2021.10.027.

Sucha, V., & Sienkiewicz, M. (2020). *Science for Policy Handbook*. Elsevier. https://shop.elsevier.com/books/science-for-policy-handbook/sucha/978-0-12 822596-7.

Tamo-Larrieux, A., Mayer, S., & Zihlmann, Z. (2021). *Not Hardcoding but Softcoding Privacy*. https://www.alexandria.unisg.ch/handle/20.500.14171/110418.

Tareke, T., & Datta, S. (2018). & IEEE. *Automated and Cloud Enabling Cyber Security Improvement in Selected Institutions/Organizations* (WOS:000589749000061). 533–538.

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law and Security Review*, *38*. https://doi.org/10.1016/j.clsr.2020.105454.

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine*, *129*. https://doi.org/10.1016/j.compbiomed.2020.104130.

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, *8*(1), 45. https://doi.org/10.1186/1471-2288-8-45.

Toli, C. A., & Preneel, B. (2018). Privacy-preserving biometric authentication model for E-finance applications. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, *2018-January*, 353–360. https://doi.org/10.5220/0006611303530360.

Urquhart, L., & Rodden, T. (2016). A Legal Turn in Human Computer Interaction? Towards 'Regulation by Design'for the Internet of Things. *Towards 'Regulation by Design'for the Internet of Things (March 11, 2016)*.

Van Cleynenbreugel, P. (2019). *By-design regulation in the algorithmic society: Promising way forward or (EU) constitutional nightmare in-the-making?* Inaugural conference of the IACL Research Group on Algorithmic State Market & Society–Constitutional dimensions.

van Gelder, P., Klaassen, P., Taebi, B., Walhout, B., van Ommen, R., van de Poel, I., Robaey, Z., Asveld, L., Balkenende, R., Hollmann, F., van Kampen, E., Khakzad, N., Krebbers, R., de Lange, J., Pieters, W., Terwel, K., Visser, E., van der Werff, T., & Jung, D. (2021). Safe-by-design in Engineering: An overview and comparative analysis of Engineering disciplines. *International Journal of Environmental Research and Public Health*, *18*(12). https://doi.org/10.3390/ijerph18126329.

van Haaften, W., Sangers, A., van Engers, T., & Djafari, S. (2020). Coping with the general data protection regulation: Anonymization through multi-party computation technology. *Jusletter IT*, 427–436. https://doi.org/10.38023/4d7c39e9-126a-4617-aebf-9bb88e9bc81f.

Vasylkovskyi, V., Guerreiro, S., & Sequeira, J. S. (2021). Designing and Validating a Blockchain-based Architecture to Enforce Privacy in Human Robot Interaction. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-January*, 566–575. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85108353955&partnerID=40&md5=851dc69d311e5e2fcc21f5c614a1001e

Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), 97–112. https://doi.org/10.9785/cri-2021-220402.

Vivarelli, A. (2020). The crisis of the right to informational self-determination. *Italian Law Journal*, *6*(1), 301–319.

Vizitiu, A., Nita, C. I., Puiu, A., Suciu, C., & Itu, L. M. (2019). Privacy-Preserving Artificial Intelligence: Application to Precision Medicine. *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, 6498–6504. https://doi.org/10.1109/EMBC.2019.8857960.

Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, *41*. https://doi.org/10.1016/j.clsr.2021.105567.

Weatherill, S. (2014). EU Consumer Law and Policy. Edward Elgar Publishing. https://www.e-elgar.com/shop/gbp/eu-consumer-law-and-policy-9781782548317.html

Yeung, K. (2017). Hypernudge': Big Data as a mode of regulation by design. *Information Communication and Society*, *20*(1), 118–136. https://doi.org/10.1080/1369118X.2016.1186713.

Yeung, K., Howes, A., & Pogrebna, G. (2019). AI governance by human rights-centred design, deliberation and oversight: An end to ethics washing. *The Oxford Handbook of AI Ethics, Oxford University Press (2019)*.

Zalloum, M., & Alamleh, H. (2020). Privacy Preserving Architecture for Healthcare Information Systems. *2020 IEEE International Conference on Communication, Networks and Satellite, Comnetsat 2020 - Proceedings*, 429–432. https://doi.org/10.1109/Comnetsat50391.2020.9328985.

Zalnieriute, M., Moses, L. B., & Williams, G. (2020). The rule of Law by Design? *Tul L Rev*, *95*, 1063.