From Privacy to Infrastructure Regulation: Rethinking the Ethical Foundations and Functions of Data Protection in the Information Age

Abstract

This article argues that data protection should be reconceptualised as a regulatory regime for data infrastructure, rather than replicating the prohibitive logic of privacy. Despite increasing recognition within European legal discourse, data protection is still widely conflated with privacy in transnational contexts. This conceptual conflation undermines regulatory coherence, erodes normative legitimacy and constrains the capacity of data protection law to address collective harms. Through a historical analysis, the article traces the divergent origins, regulatory logic, and ethical ethical underpinnings of privacy and data protection, showing that the latter operates not as a set of prohibitions, but as a governance regime designed to manage the flow of personal data in a fair, transparent, and accountable manner. Building on these distinctions, the article sets out three key policy areas for strengthening data protection as a form of infrastructure regulation: i) reframing the narrative that pits data protection against innovation; ii) shifting the focus from individual control to institutional accountability; and iii) empowering independent oversight bodies and encouraging public participation in monitoring. Such reconceptualisation is vital for developing data protection frameworks capable of confronting the transnational and systemic challenges intensified in the era of artificial intelligence.

Keywords: Privacy; Data Protection; Ethics; Data Infrastructure; Governance; Transnational Perspective

1. Introduction

The rapid development of information technologies has fundamentally transformed how personal data are collected, used, and transferred across economic and social domains (Van den Hoven 2008). Consequently, data protection law has emerged as a critical field of governance (Bennett 1992; Fuster 2014). Yet, it is still routinely conflated with the right to privacy. Much of the existing effort to address conceptual confusion is anchored in European jurisprudence or a narrow doctrinal interpretation (De Hert and Gutwirth 2006; Fuster and Gutwirth 2013). This has led to the broader social and ethical dimensions of data protection being understated, particularly in transnational contexts. In an era where data-driven systems, especially those empowered by artificial intelligence, are exacerbating power and information

asymmetries, entrenching social inequalities and eroding human agency, creativity, and mental health across national borders, this neglect has become increasingly untenable.

Drawing inspiration from emerging scholarship on data infrastructure (Cohen 2024; Bietti 2025; Dodds and Wells 2019), this article argues that data protection law can be understood as a form of infrastructure or public utility regulation. While privacy functions as a prohibitive and individual-focused right, data protection seeks to shape the broader ecosystem and the conditions under which personal data is collected, used, and transferred ethically. In pursuit of this goal, data protection operates at an infrastructural level, embedding transparency, fairness and accountability throughout the socio-technical system of data infrastructure. Reframing data protection in this way liberates it from the traditional conflation with privacy, a culturally contentious and individualistic concept (Yang and Yan 2021). It also sheds light on the broader ethical imperatives and the distinct regulatory logic of data protection law, highlighting the importance of systemic safeguards, comprehensive oversight and continuous maintenance and adaptation of the law to address challenges posed by data-driven systems.

The article proceeds in seven sections. Section 2 diagnoses the ethical mischaracterisation of data protection as privacy protection, and outlines the transnational consequences of this conceptual conflation. Section 3 examines the divergent historical roots and regulatory logics of privacy and data protection. Section 4 argues that the EU General Data Protection Regulation (GDPR) already reflects certain features of infrastructure regulation, albeit imperfectly. Section 5 critically distinguishes the ethical ethical underpinnings of privacy and data protection, emphasising the latter's focus on collective harms. Policy directions for strengthening data protection as infrastructure regulation in the age of AI are set out in Section 6. Section 7 concludes.

2. Ethical misdiagnosis and transnational implications

Privacy and data protection have long been intertwined. Many jurisdictions have named their data protection laws the "Privacy Act" or the "Information/Data Privacy Act".[1] Both academic and non-academic work often uses the terms data protection and privacy interchangeably, construing data protection as merely a subset or updated version of the right to privacy (Janofsky 2019; Borak 2021). At the heart of this conceptual conflation lies an ethical misdiagnosis with regulatory consequences. Without clearly delineating the missions and ethical values that underpin these two frameworks, we risk undermining both. The right to privacy becomes overburdened and stretched in an attempt to address systemic issues for which it was never intended. Meanwhile, data protection risks losing its legitimacy and being dismissed as a redundant clone of privacy or reduced to a set of bureaucratic procedures devoid of ethical substance (De Hert and Gutwirth 2006; Fuster and Gutwirth 2013).

The need for conceptual clarification is transnational. Within the EU, privacy and data protection have increasingly been recognised as distinct, albeit interrelated, concepts. Many European scholars had dedicated efforts to investigating the intricate relations between privacy and data protection (De Hert and Gutwirth 2009; Fuster and Gutwirth 2013; Lynskey 2014; Tzanou 2017). The GDPR, which replaced the European Data Protection Directive in 2018, moved away from explicit references to privacy, framing its objectives solely in terms of data protection (Article 1). Measures previously referred to as "privacy by design" and "privacy impact assessments" were renamed "data protection by design" and "data protection impact assessments" (Articles 25 and 35).

This conceptual decoupling in Europe, on the surface, was prompted by the Lisbon Treaty, which made the EU Charter of Fundamental Rights legally binding. The Charter recognises the protection of personal data (Article 8) as a right separate from the right to privacy (Article 7). However, this decoupling also served as a response to the decade-long legitimacy crisis confronting the EU data protection regime. Many scholars have recognised troubling discrepancies between European data protection laws and practices, and the traditional notions of privacy used to justify them (Bergkamp 2002; Burkert 2009). This was particularly evident in the regime's inability to justify its extensive regulatory scope, which covers all identifiable personal data, regardless of its relevance to privacy (Kokott and Sobotta 2013; Lynskey 2015). Some national courts had interpreted data protection provisions through the lens of privacy, declining to apply them where the processing of personal data does not explicitly infringe the right to privacy (Tzanou 2017; Lynskey 2014). The regime's ability to address collective harms is thereby undermined. Furthermore, the inclusion of regulatory elements with limited relevance to privacy, such as the principles of data quality and purpose limitation, and elements that sometimes conflict with privacy, such as data access and portability rights, has widened the gap between data protection and privacy (De Hert and Gutwirth 2009; Mostert 2018; Dalla Corte 2020).

Yet the European debates, while sophisticated and inspiring, address only part of the problem. Much of the effort to resolve conceptual confusion has focused on analysing the European courts' jurisprudence on the fundamental right to privacy and the right to protection of personal data within the EU's legal framework. However, the implications of such conceptual conflation extend far beyond Europe. As shown in comparative studies, the divergences in the conceptions of privacy across cultures and societies are remarkably complex and intractable. For example, Ess (2005) has argued that Western concepts of privacy are quite alien to China, Japan, Thailand and many other Asian countries due to their distinct cultural, historical, religious and philosophical traditions. Capurro (2005) similarly observed that many Eastern countries and African cultures "give privacy a negative connotation", while the Japanese scholars Nakada and Tamura (2005) acknowledged that "one thing is clear: privacy is not an 'intrinsic good' for us". Even after the concept of privacy was imported into Japan, it blended in a complex way with the Buddhist tradition of mushin ("denial of subjectivity") and traditional values such as aida ("the space between people") (Capurro 2005). In Thailand, the main justification for privacy is the traditional value of "saving face"; accordingly,

interference in "private affairs" is acceptable and even welcome, when conducted with the purpose of "saving face" (Kitiyadisai 2005). An anthropological study (Miller et al. 2016) further concludes that, whereas privacy debates in Europe and North America are grounded in the assumption that privacy is a natural state threatened by online visibility, this premise does not apply to China, either historically or in contemporary practice.

Against this background, conflating data protection with privacy misleadingly implies that achieving a global consensus on data protection standards is neither necessary nor feasible. However, the lack of harmonisation of data protection norms not only creates legal uncertainty and increases compliance burdens for businesses that rely on cross-border data transfers, but also potentially undermines the effectiveness of advanced data protection laws, such as the GDPR (Chander and Schwartz 2023; Yang and Yan 2021). In many Asian and African societies, where privacy is perceived as an alien or narrow concept, or as a lower priority than other traditional values (Capurro 2005; Ess 2005; Cockcroft and Rekker 2016), conflating privacy and data protection risks undermining the legitimacy, significance and practical implementation of European-style data protection laws, even when such laws are adopted to facilitate trade relations with the EU (Yang and Yan 2021). As Cockcroft and Rekker (2016) found in their quantitative research, individuals in countries with high group collectivism scores, including many in Asia, tend to take pride in their identities as members of families, communities, and organisations. This orientation often results in a lower concern for individual privacy, leading to a less rigorous approach to data protection legislation when the protection of (information) privacy is mistakenly assumed to be its primary objective. This is consistent with findings that, despite the widespread adoption of EU-inspired data protection legislation in Asia, many jurisdictions still suffer from inadequate drafting, limited enforcement and only superficial adherence to core principles (Greenleaf 2014; Greenleaf 2015; Shao et al. 2025; Igaya and Sudoh 2025). After all, extrinsic motivations alone, such as maintaining trade relations with the EU, are unlikely to foster a deep-rooted commitment to data protection regulation unless the ethical foundations of data protection — beyond Western-centric notions of privacy — become widely acknowledged.

China provides a particularly instructive example of how this conceptual conflation can migrate from theory to practice, resulting in narrow enforcement approaches and misdirected public, academic and legislative attention. For instance, even though data protection rules were introduced in various Chinese legislations in the early 2010s, many data protection cases have been dismissed by the courts on the grounds that the personal data in question is not related to privacy, or because plaintiffs cannot meet the high burden of proof required to demonstrate fault and causation in privacy tort cases (Zhou 2021). Furthermore, as privacy in the Chinese legal context is merely a civil right intended to resolve disputes between individuals and/or private entities, the conflation of concepts has led to the misconception that the recently enacted Personal Information Protection Law (PIPL) is merely a *lex specialis* of the Civil Code (Wang and Peng 2021). Consequently, private law remedies, particularly civil litigation, are considered

the primary enforcement mechanism of the PIPL, while the importance of administrative enforcement is unduly understated. By the same token, the data processing activities of government agencies are implicitly exempt from public scrutiny and academic discussion, despite the PIPL's formal applicability to both public and private sectors (Wang and Peng 2021; Sun 2022). In terms of criminal enforcement, Guo (2025) similarly argues that the conceptual conflation of privacy and data protection has led Chinese criminal law to adopt a narrow "privacy protection strategy focusing on information transfer" (p 1), which limits protection to the illegal acquisition and provision of personal information, and fails to address illegal use of personal information.

The United States represents a distinct but equally consequential manifestation of the same conceptual conflation. In the United States, freedom of expression is protected under the First Amendment to the Constitution and is not subject to proportionality analysis. When privacy and freedom of expression clash, privacy almost always loses out. Courts have often resisted regulatory interventions that impose substantive constraints on data processing in the private sector, viewing them as potential infringements on the freedom of expression (Hartzog and Richards 2020; Krotoszynski, 2016). Despite recent advances in state-level legislation, such as the California Consumer Privacy Act (CCPA), concerns remain about the potential deregulatory effect of the First Amendment on the CCPA and similar state laws (Chander et al. 2021). However, as we will explain below, privacy is only one of the many individual rights upheld by data protection law, and the processing of personal data can sometimes pose a threat to freedom of expression. Furthermore, state laws, shaped by the long-standing tradition of conflating data protection with privacy and conceptualising privacy as an individual right to control personal information, rely heavily on notice-and-choice mechanisms and individual rights (Waldman 2021; Solove 2023).

Most importantly, if left unaddressed, the conflation of privacy and data protection threatens to hinder transnational dialogue and cooperation at a critical juncture. Firstly, it perpetuates the misconception that the field labelled "privacy law" concerns only personal secrets and dignitary harms (Goldman 2023). This marginalises decades of data protection law scholarship that examines how information technologies and information about people can impact power relations and governance structures, and analyses how law can intervene to reshape them. Insights from data protection scholarship, particularly with regard to collective harms and regulatory design, are vital for addressing the complex challenges posed by the global expansion of AI technologies (Viljoen 2024). Secondly, as long as societies and academic traditions remain divided over the concept of privacy, transnational policymaking will lack a common normative foundation (Hartzog 2021). This fragmentation benefits malicious actors, particularly global technology companies, who exploit regulatory gaps and inconsistencies to expand surveillance practices with minimal accountability (Viljoen 2024). Taken together, these trends—marginalising the systemic insights of data protection law and promoting conceptual confusion—undermine collective efforts to govern the global data ecosystems effectively.

3. Diverging historical roots and missions

The persistent conflation of privacy and data protection is not merely a matter of terminology. It neglects the fundamentally different historical origins and mandates of the two frameworks. Privacy emerged in the nineteenth century in response to the need to shield individuals from unjustified intrusion. Data protection, on the other hand, arose almost a century later in response to the systemic governance challenges posed by automated data processing in the information age.

3.1 The birth and evolution of the right to privacy

Though the legal concept of privacy is rooted in older philosophical and cultural traditions (Wacks 2015), it is commonly[2] understood to have crystallised with the publication of Warren and Brandeis's famous 1890 article, "The Right to Privacy" (Wacks 2015; Kramer 1989). Motivated by the invasive practices of the press and the inadequacy of existing legal remedies, Warren and Brandeis (1890, pp 213 and 205) proposed a common law right to privacy, based on the ethical imperative to protect individuals' "dignity" and the "inviolate personality". In their eyes, privacy invasion not only results in "mental pain and distress, far greater than could be inflicted by mere bodily injury", but also involves an effect "upon his estimate of himself and upon his own feelings" (pp 196-197). In their formulation, privacy primarily functioned as a prohibitive right, a shield against unwanted intrusion into an individual's private sphere. The right to privacy is "against the world" and is "to protect the privacy of private life and to whatever degree and in whatever connection a man's life has ceased to be private" (pp 213-215). By contrast, matters or actions occurring outside this privacy zone fall outside the scope of privacy protection (pp 214 and 218).

This conceptualisation shaped subsequent legal developments. In US tort law, the Restatements (Second) of Torts (§ 652) generally limited privacy protections to intrusions that would be considered "highly offensive to a reasonable person", thereby reinforcing a narrowly defined zone of protection (Citron 2010). William Prosser (1960), the principal architect of the Restatement, recognised that complete privacy is illusory in modern society, insisting on a stringent threshold for triggering privacy claims. In constitutional law, the resemblance is unsurprising given that the first explicit claim to a constitutional right to privacy was made by Justice Brandeis himself, in his dissent in *Olmstead v. United States* (1928). Although the focus of the case shifted from the press to government surveillance, Brandeis's reasoning remained consistent, echoing the same ethical and prohibitive rationale (Glancy 1979). This significantly influenced later rulings (Solove 2002a), notably in *Griswold v. Connecticut* (1965), where the Supreme Court recognised a constitutional right to privacy and prohibited governmental intrusion into the marital bedroom. The concept of "privacy zones" since then emerged as a recurring judicial theme, reinforced by the "reasonable expectation of privacy" test established in *Katz v. United States* (1967). Consequently, US courts

routinely reject claims where the information in question has been disclosed, even when such disclosure is limited (Solove 2001).

International recognition of the right to privacy has mirrored its American origins. Articles 12 of the 1948 Universal Declaration of Human Rights (UDHR) and 8 of the 1950 European Convention on Human Rights (ECHR) enshrined privacy as a human right, primarily understood as protection against arbitrary interference. The drafting of the UDHR was influenced by the American Law Institute's 1945 Statement of Essential Human Rights, which drew on the ideas of Warren and Brandeis (Diggelmann and Cleis 2014; Humphrey 1984). It is therefore unsurprising that the characteristics of the international human right to privacy closely mirror those set out by Warren and Brandeis. From a traditional human rights perspective, privacy is "negative in nature" and constitutes a "right of non-interference", rather than a claim to positive entitlements. In terms of scope, this right only protects individuals while their personal information remains within the private sphere; once it enters the public domain, protection diminishes significantly (Prins 2006; Fuster and Gutwirth 2013).

The ethical and prohibitive nature of the right to privacy is particularly evident in Article 8 of the ECHR, which provides that any interference with private life must be justified by law and necessary in a democratic society. Accordingly, courts adopt a two-step analysis: first, whether there has been an intrusion into protected zones of privacy, and second, whether such intrusion is legally justified. Unless justified under the limited exceptions outlined in Article 8(2), interference must be strictly prohibited (Lynskey 2015). Importantly, before the Lisbon Treaty came into effect in 2009, Article 8 ECHR served as the main basis for the European data protection regime and was frequently cited in cases concerning data protection (Bygrave 1998; Lynskey 2014). However, despite the deliberate and progressive expansion by European courts over the past decades, the right to privacy is still limited in scope and defensive in nature compared to established data protection law (Lynskey 2015; Tzanou 2017). In light of these significant disparities, it is now widely accepted in Europe that data protection and privacy are two related yet distinct concepts. In short, the focus on shielding limited zones of private life from intrusion persists in both U.S. law and international human rights frameworks.

3.2 Rise of data protection in the early 1970s

Contrary to the relatively long history of the right to privacy, the concept of data protection only emerged in the late 1960s and early 1970s. A common catalyst for the emergence of data protection law in European countries during this period was the establishment or planned introduction of centralised, computerised population databases by governments (Bennett 1992). As Hustinx (2014), the then European Data Protection Supervisor, stated in 2014, the concept of data protection was created four decades ago, in order to provide legal protection for individuals against the inappropriate use of information technology to process information relating to them.

This statement is affirmed by Hondius (1980), a pioneering data protection scholar, who noted that the concept of data protection hardly existed just 12 years before.

According to an extensive historical review, the English "data protection" may have originally been borrowed from the German "Datenschutz" (Fuster 2014; Hondius 1980). The first legal instrument to bear the name of Datenschutz was the Hessian Data Protection Act promulgated by the German state of Hesse in 1970. It was also the world's first-ever data protection law (Hondius 1975; Wacks 2015). The Hessian Data Protection Act defined Datenschutz, the term that was later translated into English as "data protection", as "the obligation for records, data and the results attained by their processing to be obtained, transmitted and stored in such a way that they could not be consulted, altered, extracted or destroyed by an unauthorized person" (quoted in Fuster 2014, p 57).

The concept Datenschutz had since gained popularity in Germany and been used all over Europe. In 1974, Rhineland-Palatinate, another state of Germany, adopted a data protection law that referred to Datenschutz in its first article and deployed its remaining provisions around the concept (Hondius 1975). Also, the Hessian Data Protection Act was discussed extensively during the preparation of the 1973 Swedish Data Act, the world's first national data protection law (Bennett 1992). The Swedish Act was translated into English, French and German and was later used as exemplar in many European countries' data protection legislation (Bennett 1992; Hondius 1975). In 1977, Germany enacted its first federal data protection law, Bundesdatenschutzgesetz, which not only endorsed the concept of Datenschutz, but also included a comprehensive range of interests and values that might be affected during personal data processing (Hondius 1975).

Importantly, while various European countries began enacting laws to regulate the processing of personal data in the 1970s, these early national data protection laws were rarely associated with anything resembling privacy (Fuster 2014). In the mid-1970s, experts at the Council of Europe declared that the body of laws that were emerging across Europe for the protection of individuals against computerised records had already acquired a name of its own: "data protection" (Fuster 2014). The novel European concept of data protection, as Hondius (1980, p 90) noted "has a wider meaning than the American concept of privacy".

Shortly after the emergence of data protection law in Europe, the US also adopted its data protection law, namely, the US Privacy Act 1974. In contrast to the early data protection laws of European countries, the US Privacy Act, as its title suggests, was expressly based on privacy. This is largely attributed to the fact that in the late 1960s, several influential US scholars framed the issue of regulating personal data processing in the face of technological development as an extra dimension of privacy (Fuster 2014, p 48). Most famously, Westin (1967) reconceptualised privacy as information control. However, despite its nominal continuity with privacy, many scholars have recognised

that the so-called new strand of privacy, i.e. informational privacy, is very different from, and even in tension with, traditional privacy concerns (Solove 2002a, 2002b; Post 2017). In fact, in his later work, Westin himself has recognised that there are two fundamental principles governing the processing of personal data, namely, due process and privacy, with the value of due process being entirely independent of privacy (the right to be left alone) (Mahieu 2021). Not surprisingly, it is argued that despite a long history of concern about the right to privacy in the US, when American policymakers sought to develop public policies to mitigate the dangers of information technology, they were actually looking for new solutions to new problems (Bennett 1992). The subsequent, and widely accepted conflation of data protection and privacy is essentially the result of a series of "mistranslations" and "miscommunications" in legal history (Fuster 2014).

3.3 From prohibition to infrastructure regulation

The historical divergence between privacy and data protection has led to distinct regulatory logics. As mentioned above, the first-generation data protection laws that emerged in the 1970s were not designed to prohibit the state's use of personal data outright. Instead, they sought to establish the conditions that government-initiated data-driven systems had to fulfil. This origin reveals non-prohibitive as a foundational and inherent feature of data protection. As Advocate General Siegbert Alber of the Court of Justice of the European Union observed, "there would be no need for data protection if a general prohibition on data processing were the normative baseline" (Case C-369/98 2000, Opinion of AG Alber, para 41).

Recognising such non-prohibitive nature, however, does not entail a laissez-faire approach. Data protection functions as a form of infrastructure regulation, which establishes a framework of procedural requirements, substantive norms, and organisational safeguards, thereby embedding fairness, transparency, and accountability into data ecosystems. A key early illustration of this regulatory logic is the landmark Census decision of the German Federal Constitutional Court (Bundesverfassungsgericht 1983). In response to public concern about the proposed population census, the Court ruled that the Census Act was partly unconstitutional. In its reasoning, the Court has articulated the constitutional right to informational self-determination, which later formed the basis of German data protection law and subsequently the EU regime. Rather than prohibiting the census, the court has mandated an assessment of its legality and necessity, as well as a wide range of procedural and organisational safeguards. These include the context-sensitive application of purpose limitation and data minimisation; the appointment of independent regulators to ensure precautionary legal protection; and the requirements to notify, delete and anonymise data in certain circumstances. Then, in 1985, a revised Census Act was passed, and the census proceeded in 1987, demonstrating the logic of reconfiguring the infrastructure rather than banning it outright (Hornung and Schnabel 2009; Schwartz 1989).

This regulatory logic has largely persisted in the European data protection regime. For

instance, while the 1995 Data Protection Directive is primarily recognised for safeguarding individual privacy, it is also aimed to facilitate the free movement of personal data between Member States, thereby supporting the development of the internal market and harmonising protective standards across the EU.[3] The GDPR, which replaced the Directive in 2018, also pursues two objectives: protecting individuals' rights and freedoms, and ensuring the free flow of personal data within the EU.[4] In other words, the regime is concerned not only with mitigating the risks of data misuse, but also with enabling the legitimate and ethical use of personal data. The impact of the Directive and the GDPR on data protection legislation worldwide is well recognised (Birnhack 2008; Schwartz 2019).

This shift from prohibition to infrastructure regulation reflects the realisation that the risks associated with automated and large-scale data processing cannot be managed through prohibitive or reactive rules alone. The prohibitive nature that makes the right to privacy powerful also limits its capacity to address the systemic risks in the information age. As illustrated above, privacy presumes the existence of a defined private sphere, and functions effectively when those boundaries are violated. However, modern data processing rarely operates through discrete intrusions. Instead, it often operates invisibly, aggregating fragments of disclosed or publicly available data, drawing inferences, categorising individuals and influencing behaviours without triggering traditional privacy thresholds (Zuboff 2019b; Cohen 2019). If information has already been shared, if there has been no clear intrusion into zones of privacy, or if the harm is collective rather than borne by specific individuals, the right to privacy tends to become impotent. Attempts to stretch the right to privacy to cover all these issues risk diluting its normative force. In other words, if privacy comes to mean everything, it may ultimately mean very little. The prohibitive function of privacy risks being lost in a flood of data protection problems that it was never designed to handle (De Hert and Gutwirth 2006; Fuster and Gutwirth 2013).

In summary, privacy and data protection emerged in different historical contexts in response to distinct regulatory challenges, and have different functions. Blending them together risks undermining both, diminishing privacy's role in defending personal boundaries, while obscuring data protection's function as infrastructure regulation in the governance of data ecosystems.

4. Data protection as infrastructure regulation

As indicated above, data protection does not prohibit the processing of personal data outright; rather, it functions more accurately as a form of infrastructure or public utility regulation. This reconceptualisation draws from a growing body of scholarship that conceptualises data as a form of infrastructure (Cohen 2024; Bietti 2025; Dodds and Wells 2019), grounded in Brett Frischmann's influential definition of infrastructure. According to Frischmann (2012), infrastructures are resources characterised by non-rivalrous (or partially non-rivalrous) consumption, broad social demand for enabling

downstream productive activities, and their function as inputs into public and private goods and services used by a wide range of users across society. Building on this definition, scholars such as Cohen (2024), Bietti (2025) and Dodds and Wells (2019) have recognised that data meets all of these criteria: it is non-rivalrous in that multiple actors can use the same data simultaneously; it is widely demanded to fuel algorithmic processes, platform operations, and digital communication; and it serves as a foundational input across sectors. Therefore, viewing data as infrastructure is not just an analogy; it reflects its importance and functional role in coordinating social and economic activity and driving innovation in the information age.

More importantly, this perspective enables the insights gained from the governance of traditional infrastructure over time to inform data governance. As Cohen (2024) notes, viewing data as infrastructure implicates a very different regulatory tradition. Regulatory regimes for traditional infrastructure and public utility generally focus on managing the flow of human activity and exchange at various levels, with regulators playing a direct role in representing the public interest. Conceptualizing data as infrastructure, therefore, requires shifting from the current regulatory approach, which prioritizes *post-hoc* interventions, towards mechanisms that assert public interests more directly and engage with data-driven operations at an infrastructural level.

The infrastructural feature and function of data determine that it must be governed in the public interest, regardless of who *de facto* creates, owns and controls it (Bietti 2025). Granting individuals a veto right, while important, cannot address collective concerns alone. In response, Bietti (2025) advocates an infrastructure-based approach to data governance, shifting the focus away from individual control mechanisms, such as consent and data subject rights, towards "structuring flows and data pipelines" to enable "more effective collective self-determination" (p 71). Dodds and Wells (2019) argue that, just as societies make great efforts to plan for, invest in and maintain the physical infrastructure they rely on, we must apply the same level of commitment to the governance of data infrastructure. Importantly, we must incorporate openness and trustworthiness into data infrastructure to maximise its long-term social and economic value. This can be achieved by "build(ing) ethical considerations into how data is collected, managed and used" across the entire data ecosystem, and enabling "meaningful engagement with organisations and people" who could be affected by data processing (p 267).

Building on these insights, this paper argues that data protection law should be understood as a regulatory regime for data infrastructure, rather than as an extension of the right to privacy. Much like a well-regulated transport system, with its hierarchy of motorways, cycle lanes, no-traffic zones, driver licensing system, vehicle checks and maintenance documentation, roadside inspections and post-incident enforcement, an effective data protection framework must coordinate diverse data flows, allocate responsibilities across actors, impose calibrated constraints and exceptions, ensure real-

time compliance monitoring and provide sanctions and remedies when harms to individuals or society occur.

The logic of infrastructure regulation has been reflected in the foundational architecture of the GDPR, albeit in a nascent form. To begin with, the GDPR organises the flow of personal data through a wide range of legal bases for processing (Article 6) including consent, contractual necessity, legal obligation, vital interests, public tasks, and legitimate interest. Importantly, unlike the right to privacy, the GDPR applies to all personal data, regardless of whether the information has been shared or is publicly available. For sensitive personal data, the threshold is reinforced by the heightened protection requirements set out in Article 9. The framework is further modulated by targeted exemptions, such as those for scientific research, statistical analysis or purely domestic activities. Like motorways, cycle lanes, and pedestrian crossings in a transport network, each legal pathway facilitates data movement under defined conditions, calibrated to the varying levels of scrutiny and protection appropriate to different types of processing.

Secondly, the GDPR establishes a set of principles governing the entire lifecycle of data processing. These principles act as constraints within the broader and generally permissive architecture of data infrastructure. At the heart of these is the fairness principle (Article 5(1)(a)), which requires data controllers to process personal data lawfully and transparently, and to assess and ensure a fair balance between their own legitimate interests and those of the data subjects. Likewise, the purpose limitation principle (Article 5(1)(b)) constrains the use of personal data for purposes other than those originally intended, while the storage limitation principle (Article 5(1)(e)) restricts the indefinite retention of data, contributing to the broader aims of foreseeability and fairness. By restricting ethically problematic data processing and defining “no traffic zones”, these principles help to cultivate a fair and ethical data ecosystem.

Thirdly, the GDPR has introduced an accountability regime to ensure that data controllers and processors not only comply with legal obligations but also be able to demonstrate such compliance. To fulfil the accountability principle (Article 5(2)), organisations are required to implement several measures, such as data protection impact assessments (Article 35), and record keeping (Article 30). These mechanisms resemble the requirements for driving licenses and vehicle maintenance records in traffic regulation, functioning both as conditions for lawful operations and as evidence of an ongoing commitment to regulatory compliance. Articles 33 and 34 require organisations to report data breaches within 72 hours and notify affected individuals when their rights are at risk, akin to post-incident reporting duties in the traffic context. The requirement for data protection by design and by default (Article 25) means that accountability must extend to the system design and default-setting stages, similar to the infrastructure planning and approval processes, which aim to proactively filter out foreseeable hazards rather than react to them.

Additionally, the GDPR establishes a multi-layered oversight framework to monitor and enforce compliance at institutional level. Similar to the roles of licensing authorities, the transport police and the courts in the transport regulatory system, these multiple forms of oversight perform complementary functions throughout the data infrastructure. Data Protection Officers (DPOs) ensure continuous internal compliance and provide advisory support; Data Protection Authorities (DPAs) investigate breaches and impose sanctions; and courts provide avenues for individual redress and compensation.

Nevertheless, the GDPR is not without its limitations. There are persistent criticisms regarding the disproportionate compliance costs and burdens placed on small and medium-sized enterprises (SMEs) (Gal and Aviv 2020; European Commission 2024). DPAs in some member states are overloaded and under-resourced, with limited capacity to conduct proactive oversight or engage meaningfully with complex cases (European Commission 2020; FRA 2024). However, these limitations do not undermine the value of the infrastructural perspective or the importance of the data protection law itself; rather, they reinforce both. Under-resourced and politically constrained DPAs expose the infrastructural need for sustained investment in regulatory capacity and institutional independence. The disproportionate burden on SMEs highlights the distributive equality issue that must be carefully considered in any infrastructure regulation.

This reconceptualisation offers several analytical and normative advantages. It reorients data protection away from an overly individual-focused perspective and towards broader social and ethical considerations. Moreover, it sheds useful light on the regulatory logic of the field: the focus is not on restriction per se, but on enabling socially beneficial and ethically responsible data processing. It also underscores the need for systemic safeguards and comprehensive oversight to manage the multifaceted, diffuse risks of modern data-driven systems, as well as the importance of ongoing investment in regulatory capacity and institutional adaptability as technology advances and data infrastructure evolves. Finally, recognising data as infrastructure underscores the need for transnational coordination and legal harmonisation. Just as traditional infrastructures such as telecommunications and transports depend on international coordination and agreed standards to ensure seamless connectivity and continuous operation (GIH 2021), data infrastructure, built on transnational flows and distributed architectures, cannot be effectively governed by national laws in isolation (ODI 2023). Therefore, viewing data protection as infrastructure regulation not only helps to define its domestic function more accurately, but also highlights the urgent need for regulatory frameworks capable of responding to the cross-border and systemic challenges of today's interconnected digital world.

5. Ethical foundation and collective focus of data protection

As established in the previous sections, privacy and data protection emerged in different historical contexts with different regulatory objectives. Privacy, as a prohibitive right, aims to protect the individual from dignity-related harm by shielding a sacred zone of non-intrusion. By contrast, data protection arose from the realisation that, even without violating private zones, automated data processing in the information age can generate profound harm at both the individual and societal levels. This section further elaborates on their ethical divergence by first identifying privacy's place among the ethical underpinnings of data protection, and second exploring data protection's orientation towards societal-level harms.

5.1 Privacy and other individual rights underpinning data protection

While data protection law is often misunderstood to be a legal instrument whose fundamental purpose is to protect individuals' right to privacy, the ethical considerations of data protection law are far broader and more diverse. As Bygrave (2001; 2002) notes, while data protection law is, to some extent, concerned with safeguarding individual privacy, it would be wrong to infer that it is solely concerned with privacy. Some even argue that data protection should be viewed as a "bundle of rights that make up citizenship in the new millennium" (Rodotà 2009, p 80). Although this view is more prevalent in European scholarship, it also appears to be implicitly held by some leading academics in other jurisdictions. For example, American scholar Daniel Solove (2005) has repeatedly stressed that data processing increases not only the risk of digital harm to individuals, but also the risk of them suffering various monetary and physical harms. Similarly, Hartzog and Richards (2020, p 495) argue that data protection is about "civil rights, free expression, freedom from harassment and collective autonomy interests".

Among all the non-privacy-related individual rights that underpin data protection, the right not to be discriminated against is most prominent. The EU data protection regime and most national laws influenced by it impose additional requirements on the processing of sensitive data. Although some of the data classified as sensitive fall within the domain of privacy, the link between this provision and the right not to be discriminated against is equally, if not more, prominent (Lynskey 2015; Gellert and Gutwirth 2013). In its guidance, the Article 29 Working Party explicitly recognises that the rationale behind regulating certain categories of data differently is based on the assumption that the misuse of these data could have more severe consequences for the individuals' fundamental rights, including the right to non-discrimination (WP29 2011). The GDPR not only removes the emphasis on the right to privacy, but also explicitly lists discrimination as one of the potential harms that can be caused to individuals by the misuse of personal data (Recitals 75 and 85).

Another important underlying value is freedom of expression. Recital 4 explicitly affirms that the GDPR respects not only the right to privacy, but also freedom of expression and information, freedom of thought, and so on. This position has also been demonstrated in several decisions by the European courts. For example, in the joint

cases of *Tele2/Watson*, the Court of Justice of the European Union (CJEU) found that legislation obliging providers of electronic communication services to retain traffic data raised questions relating not only to the right to privacy in Article 7 of the EU Charter of Fundamental Rights, but also to the freedom of expression in Article 11 of the Charter. Similarly, in *Segerstedt-Wiberg v Sweden* (2006), where data subjects' requests for access to records held by the Swedish Security Police were refused on the grounds that disclosure might endanger national security, the ECHR recognised that the Police's storage of personal data relating to political opinions and affiliations interfered with the right to privacy as well as freedoms of expression and association. Nevertheless, most data protection discussions to date, especially outside Europe, still focus overwhelmingly on the right to privacy and largely neglect freedom of expression, which in turn can deter the development and implementation of data protection law in jurisdictions such as the US.

To sum up, while privacy is an important right and ethical consideration in data protection, it is neither the only concern nor necessarily the most relevant one. Conflating data protection with privacy risks obscuring the broader range of rights and freedoms implicated in the processing of personal data. Consequently, rights and freedoms beyond the right to privacy may be underrepresented in data protection discussions and enforcement.

5.2 Data protection's concern for collective harms

While privacy is often concerned with remedying dignitary harms to specific individuals, data protection focuses more on the long-term negative implications of the automated processing of personal data for society as a whole. One indication of this orientation is that the original regulatory target of data protection law was automated data processing. According to Fuster (2014), "Datenschutz" the German origin of data protection, specifically refers to data undergoing automated processing, as opposed to data in general. Many of the early international data protection instruments, such as the Council of Europe's Resolution 73 (22), Resolution 74 (29), and Convention 108, all focus on the automated processing of personal data and exclude manual processing. This regulatory orientation reflects an early recognition that automated processing of personal data can result in collective harms that cannot be adequately addressed by traditional privacy rights, which primarily focus on remedying individual-level harm.

Although many subsequent data protection laws, including the European Data Protection Directive and the GDPR, have extended their regulatory scope to cover certain manual processing of personal data in order to prevent circumvention of the laws, closer inspection reveals that they still place a greater regulatory focus on automated and large-scale processing of personal data, as opposed to manual and one-off processing. For example, the Directive does not require the notification of purely manual processing of personal data to the supervisory authority, whereas this is mandatory for wholly or partially automatic processing (Article 18). Likewise, Article 22 of the GDPR grants data subjects the right not to be subject to a decision based solely

on automated processing (including profiling) where that decision produces legal effects concerning the data subject or similarly significant effects on them. Article 37 requires the appointment of a Data Protection Officer (DPO) where data controllers' core activities involve regular and systematic monitoring of data subjects on a large scale, or large-scale processing of special categories of data or data relating to criminal convictions and offences, or where the controller is a public body.

Importantly, many societal problems generated by contemporary data processing are, or should be, a primary concern of data protection law, yet cannot be adequately captured by the right to privacy. As Zuboff declared, "We've entered virgin territory here. The assault on behavioural data is so sweeping that it can no longer be circumscribed by the concept of privacy and its contests" (Zuboff 2016). Solove (2023) has also recently acknowledged that "privacy issues extend beyond threats to individual privacy", and that the misuse of personal data can cause broader societal problems. Against this background, we argue that the processing of personal data in the current information age has resulted in at least three clusters of societal problems that extend beyond the scope of privacy issues: (1) the deepening of information and power asymmetries; (2) the proliferation of social sorting that contribute to systemic inequality and the marginalisation of vulnerable groups; and (3) the modulation and erosion of human agency, creativity and mental wellbeing.

As discussed below, these clusters are neither exhaustive nor mutually exclusive, but are interrelated and sometimes overlap. For example, both social sorting and behavioural modulation rely on, and reinforce underlying information and power imbalances between ordinary people and powerful data controllers. Social sorting is frequently used in the modulation process by surveillance capitalists and may inhibit collective rebellious action by fragmenting affected groups, thereby compounding existing power imbalances. This section's aim is not to offer a comprehensive taxonomy of collective harms, but to map out a preliminary conceptual terrain of these interconnected collective harms, thereby prompting the development of more targeted and effective regulatory responses.

(1) Aggravation of information asymmetry and power imbalance.

The concerns raised by the pervasive processing of personal data extend well beyond the right to privacy; they also implicate broader issues of power relations and asymmetrical access to information resources and databases (Andrejevic 2007; Andrejevic 2008). As Solove (2001; 2005) contended, the problems caused by data processing in the modern age are less about the overt insult or reputational damage to an individual, and more about upsetting the balance of institutional and social power in undesirable ways. Companies are not just compromising the dignitary interests in our personal data, but also turning our data into a power capable of controlling people and institutions (Hartzog and Richards 2020). In fact, the main rationale behind the EU

Charter's recognition of a separate right to data protection is exactly to address the "non-privacy related concerns such as power asymmetry" (Lynskey 2014).

These asymmetries generate a pervasive sense of disempowerment within society. Solove (2001) describes today's data environment as a Kafkaesque world of bureaucracy, where individuals lack meaningful control over how their data is used. They struggle to assess risks, give informed consent or negotiate fair terms, which makes them vulnerable to error, such as data inaccuracies, leaks and abuse by data controllers. Meanwhile, these asymmetries obstruct both individual redress and institutional accountability. Data misuse often goes undetected as individuals cannot identify the responsible parties or comprehend the basis on which they are profiled or scored (Yeung 2018). Even regulators face challenges in identifying and addressing discriminatory or manipulative practices, given the scale and technical sophistication of contemporary data-driven systems (Raab and Szekely 2017).

(2) Social sorting and marginalisation of vulnerable groups

A second cluster of collective harm relates to social sorting and the amplification of social inequality. While it is difficult to convey that privacy is not the only concern, the most effective approach is to shift the focus from "a singular concern with privacy" to "social sorting", a problem that goes beyond the individual realm (Lyon 2010, p 115). In other words, personal data is increasingly being collected and used to categorise populations, enabling different groups to be treated differently (Lyon 2003; Lyon 2019). Social sorting often escapes traditional anti-discrimination frameworks, as it does not always target protected characteristics or operate through legally cognisable categories of inequality (Matzner and Mann 2019).

Although social sorting may occasionally serve neutral or even beneficial purposes, it very often reinforces pre-existing patterns of marginalisation (Lyon 2019; Stoddart 2014). A well-documented historical example of this is the use of colonial identity cards in Rwanda to identify the Tutsi minority for persecution and genocide (Lyon 2019). A more recent, albeit less extreme, example is the deployment of crime mapping tools by the British police to categorise neighbourhoods based on perceived crime levels. Over time, this spatial stratification can lead to differential access to services, variable insurance premiums, shifts in property values and entrenched cycles of disadvantage (Rauhofer 2014). In commercial contexts, social sorting usually leads to the preferential targeting of high-value individuals ("cherry picking") and the systematic exclusion or exploitation of those deemed less profitable ("lemon dropping") (Yeung 2018). The cumulative effect is that vulnerable populations are not only categorised, but also increasingly confined within digital architectures that shape, limit and often diminish their life chances.

(3) Modulation and Eroded Human Agency

Modulation[5] refers to a mode of data processing aimed at producing tractable, predictable citizens and consumers whose apparent choices unfold along commercially profitable trajectories (Cohen 2013). It is closely linked to the rise of surveillance capitalism over the past two decades. Dominant platforms such as Google and Facebook have amassed vast wealth by unilaterally appropriating human experience as raw material and transforming it into behavioural data and predictive products for commercial gain. This process involves not only the extraction of data, but also the modification of human behaviour — a systematic form of behaviour shaping designed to optimise engagement and profit (Zuboff 2019b; Cohen 2019).

Citizens who are constantly subject to modulation are no longer the autonomous agents envisaged by liberal democratic theory, because their preferences are largely shaped by modulation rather than being formed through robust and open debates (Cohen 2013). It is well documented that Facebook and Cambridge Analytica were deeply involved in both the UK's Brexit referendum and the 2016 US presidential election (Lapowsky 2019). In other words, while the purpose of modulation is to generate profits and appears apolitical, it can seriously undermine the functioning of political systems in liberal democratic societies. In the long term, the provision of tailored information in the modulation process also creates "filter bubbles" or "echo chambers", preventing people from being exposed to information that challenges their opinions, assumptions, and existing biases (Spohr 2017; Cinelli et al. 2021). As a result, opportunities for dialogue and the ability to reach common ground among diverse political groups are weakened, whereas ideological polarisation and social division are likely to intensify.

However, it would be a mistake to assume that the negative impact of modulation is only experienced by liberal democratic societies. People living in modulated societies will also gradually lose the ability to formulate and pursue meaningful agendas that allow them to flourish (Cohen 2013; Yeung 2016). This includes their capability to innovate. Innovation requires critical perspectives, an independent mindset, and the intellectual freedom to experiment with new ideas. In a modulated society people's subjectivity is predominantly directed along relatively linear and predictable trajectories designed by powerful companies for profit-making purposes. Consequently, pathways to serendipity and innovation are frequently obstructed (Cohen 2013). Moreover, the products and services offered by the surveillance capitalists are often designed to be addictive in order to keep users' attention and data flowing, which means that people's mental health is also at risk (Hartzog and Richards 2020). In short, modulation not only jeopardises the political foundations of liberal democracies, but also adversely affects intellectual development and mental well-being across all societies.

The foregoing discussion, however, invites a possible objection: namely, that these collective harms might be fully accommodated within an expanded concept of privacy,

rather than supporting the need for a distinct concept of data protection. Many scholars, particularly in the US, have over recent decades argued for the social importance of privacy and criticised the understanding of it as individualistic. Nevertheless, most scholars agree that the traditional and dominant understanding of privacy is still an individualistic one. For instance, Regan (1995) states that "privacy inheres in the individual as an individual" and is important primarily for personal self-development and intimate relationships. Likewise, Cohen (2013) notes that privacy theory is rooted in the tradition of liberal individualism which led to the conventional understanding of privacy as protection of the self. Westin (1967), while recognising that privacy serves a broader social function in liberal democracies, ultimately anchored his conceptualisation of privacy in the individual and the individual's relationship with society.

Importantly, the social turn in privacy scholarship has itself largely been driven by the rise of modern data processing practices. Scholars have sought to expand privacy mainly because the conventional understanding of it as an individual right has been found to be inadequate in addressing the wider implications of data processing in the information age. For example, when theorising about the social importance of privacy, Regan (1995) took her point of departure from the problem that the conventional understanding of privacy as an individual right "provides a weak basis for formulating policy" to protect people against modern threats such as database surveillance and electronic eavesdropping. Cohen (2013)'s discussion of the social values of privacy focuses primarily on the implications of data processing by private and state actors in the era of informational capitalism. While Nissenbaum (2009, p 4) admits that privacy was initially used as the organising principle to define the scope of her book due to its historical importance, she deliberately chose to frame her central claims in terms of"personal information flows", thereby shifting attention away from privacy's conceptual ambiguities and towards the governance of data processing practices.

In the meantime, a number of scholars have recognised that this expansion has generated significant conceptual tension. Simitis (1987) observed that modern information processing has altered the privacy debate in many ways. In particular, privacy concerns no longer arise out of particular individual problems, but rather express conflicts that affect everyone; and modern information processing is not about disclosing intimate information about individuals, but is an essential element of long-term strategies of manipulation designed to shape and adjust individual behaviour. Solove (2002a, 2004) distinguished the traditional "secrecy paradigm" of privacy, concerned with protecting a hidden private sphere, from contemporary privacy concerns relating to the use, sharing, and aggregation of personal data, regardless of whether that information remains secret. Similarly, Cohen (2013, 2019) recognised that, whereas traditional privacy focused on shielding individuals from exposure, contemporary privacy frameworks centre on consent as a mechanism for managing pervasive, networked interactions. More explicitly, Post (2017) drew a distinction

between “dignitary privacy” and “data privacy”, the latter being concerned with transparency, accuracy and accountability in data processing.

The social turn in privacy scholarship thus reflects the increasing pressure placed on privacy by the collective harms and systemic risks generated by modern data processing. Yet treating this move as a simple expansion or updating of privacy carries significant conceptual and regulatory costs. It may erode the prohibitive force of the right to privacy and divert it from its core function (De Hert and Gutwirth 2006; Bygrave 2001), while further stretching the already contested concept and thereby complicating transnational efforts to develop clearer and more coherent data protection standards (Yang and Yan 2021). The better reading, in our view, is therefore not that privacy should simply absorb these developments, but that the social turn in privacy scholarship reveals the limits of privacy as the organising concept for the collective harms and systemic risks generated by contemporary data processing. Many of the concerns now framed as part of privacy’s social dimension are more coherently understood as data protection concerns. A clearer understanding of what is at stake is crucial for legislators and regulators around the world to identify the issues that need to be addressed and the best approaches to tackle them. Conversely, continuing to subsume all such concerns under the single concept of privacy, a concept that is historically and conventionally understood as individualistic, risks reinforcing a narrow regulatory focus on increasing individual control. It is therefore preferable, this paper suggests, to regard privacy’s individualistic orientation not as antiquated or mistaken, but as a defining characteristic of privacy, while recognising that the broader social concerns identified by contemporary scholars pertain more appropriately to the concept of data protection.

6. Aligning data protection with its broader ethical mandates

Recognising and correcting the ethical misdiagnosis that conflates data protection with privacy is not just an academic refinement; it is an essential step towards more targeted legal responses and effective regulatory governance. This is particularly important in the age of AI, when the scale, opacity and autonomy of data-driven systems, as well as the systemic risks they pose, are increasing dramatically (Yadav and Suryadevara 2023; Sartor and Lagioia 2020). This section outlines three key policy recommendations to better align data protection law with its broader ethical mandates and infrastructural regulation function, thereby enhancing its effectiveness in governing increasingly powerful data-driven systems.

6.1 Reframing the innovation vs. data protection narrative

A recurring narrative, particularly prevalent in global industry discourse, frames data protection as a barrier to digital innovation and societal progress. This misconception has repeatedly been exploited by technology companies to lobby against the adoption

of robust data protection laws in many countries (for example, McQuinn and Castro 2019; Shen 2019), and has even led courts in some jurisdictions to override existing data protection rules.[6] Such framing fundamentally misrepresents the purpose and regulatory logic of data protection law. As shown in foregoing sections, data protection law has never sought to impose a general prohibition on the processing of personal data or the use of information technologies; instead, its purpose is to promote transparency, fairness and public accountability of data processing, thereby making them legitimate and more acceptable to the public. Data protection law recognises that data processing can yield significant societal benefits, such as increased productivity, economic development, improved public governance, but can also pose substantial risks to both individuals and society as a whole. In short, social values lie on both sides of the equilibrium.

A more accurate way to understand data protection law, accordingly, is to see it as ensuring the sustainability of data infrastructures by incorporating ethical considerations into the entire system and securing their public trustworthiness. Some scholars have drawn an analogy between the functions of data protection law and sustainable development policy in environmental law, which aims to preserve ecosystems while enabling economic growth (Bygrave 2001; Zuboff 2019b). Both regulatory regimes are based on the idea that seemingly conflicting social values can be reconciled and both immediate and future interests can be safeguarded through sound governance. Early analysis of GDPR's implementation supports this position, suggesting that the framework not only benefits individual consumers and collective well-being, but may also foster innovation, particularly in sectors where public trust is essential for adoption (Niebel 2021). This view resonates with the infrastructural perspective discussed earlier: data protection law governs data processing and coordinates data flows through a regulatory regime that promotes both openness and trustworthiness, reconciling the current societal benefits with the long-term preservation of collective well-being and individual rights.

Hence, the appropriate direction is neither deregulation nor restriction, but better regulation. A well-designed data protection law can foster responsible innovation by incorporating safeguards that strengthen public trust, ensure institutional accountability and support long-term societal progress. This reframing serves not only to correct industry misconceptions and encourage legal compliance, but also to guide the future policy development in ways that are both innovation-friendly and ethically grounded. Recent debates and reform initiatives concerning the GDPR, particularly proposals for more nuanced, risk-based and proportionate obligations, the wider use of standardised compliance tools, and the simplification and increased coherence between the GDPR and other EU digital laws to eliminate duplication and overlapping obligations, can be understood as steps in this direction (European Commission 2025; IAPP 2025).

6.2 From individual control to institutional accountability

Building on the foregoing reframing of data protection as a governance framework for sustainable and legitimate data infrastructures, a key policy shift is urgently required: to move away from an overreliance on individual control mechanisms, such as notice and consent and data subject rights, towards institutional accountability for the systemic governance of data ecosystems. As Bietti (2025, p 73) argues, an infrastructural understanding of data protection demands a move "beyond individual veto rights models" and calls for refashioning the normative grammars that technology companies have inscribed into their data processing practices. This shift does not mean abandoning the notice and consent, or data subject rights. Instead, it requires resituating them within a broader accountability architecture in which responsibilities are concentrated in institutions capable of shaping and correcting data ecosystems.

Current data protection frameworks, particularly in the United States and many Asian jurisdictions, remain predominantly "consent-centric", despite enduring information asymmetries and power imbalances that render meaningful consent largely ineffective (van Ooijen and Vrabec 2019; Graef and van der Sloot 2022; Solove 2023; Future of Privacy Forum 2021; Han 2021). This legal reality is striking, given that concerns about power imbalances have been a part of data protection law since its inception in the early 1970s. As noted above, the early legislative and judicial efforts were mostly driven by the rise of large-scale data processing by government agencies and the inherent power imbalances between governments and individuals. Mahieu (2021) has demonstrated in his genealogical account of the right of access that this key element of data protection law was conceived not merely to empower individuals, but to enable collective oversight and redress in the face of systemic power imbalances. Nevertheless, that foundation was gradually overshadowed by the prevailing conceptual conflation of data protection with privacy. As Andrejevic (2007) pointed out, "the notion of privacy does not take into account the power relations that structure the choice".

As data-driven systems become increasingly complex, opaque and powerful with the help of AI, it is both unreasonable and unrealistic to expect individuals to evaluate and manage the collective risks posed by such processing. Regulatory efforts, therefore, must prioritise institutional accountability and the regulation of broader data ecosystems. The EU's GDPR has already incorporated several underutilised mechanisms that could facilitate this shift. These include the principles of fairness and accountability, as well as tools such as data protection impact assessments (DPIAs) and data protection by design and by default requirements. When enforced rigorously, these provisions help to reallocate responsibility towards data controllers and embed regulatory norms directly into technical and organisational infrastructures, thereby reducing overreliance on individual control (Lynskey 2015; Yeung and Bygrave 2022). For example, data protection by design and by default, enshrined in Article 25 of the GDPR, if interpreted as requiring "hard" privacy-enhancing technologies rather than "soft" procedural measures, can help to embed data minimisation as an architectural

constraint rather than a voluntary policy commitment of data controllers (Rubinstein and Good 2020).

In addition to existing measures, scholars have proposed a range of complementary reforms to further increase institutional accountability and mitigate systemic risks. These include imposing fiduciary-like duties on data controllers to prevent self-interested or exploitative practices (Richards and Hartzog 2020; Balkin 2020; Tuch 2020). DPIA frameworks could be enhanced to systematically assess societal and collective dimension of risks, which often fall outside the scope of individual rights-based models (Mantelero 2018). To avoid the one-size-fit-all trap, differentiated regulatory approaches can be used to target distinct data protection problems. This may involve distinguishing between semantic (meaning-driven) and syntactic (meaning-agnostic) data processing, and enabling targeted, sector-specific regulation (Purtova and Newell 2025). Overall, these proposals converge on the need to re-centre data protection on infrastructural governance beyond individual control, by requiring institutional accountability and system-level mechanisms capable of shaping data infrastructures ex ante and correcting them ex post.

6.3 Enhancing and broadening oversight mechanisms

A third essential policy direction for reconfiguring data protection as a form of infrastructure regulation is to consolidate and democratise oversight. Legal principles and rules alone, no matter how sophisticatedly drafted, cannot address the systemic governance challenges and technical complexities of data ecosystems. Their practical effect depends on the capacity of the oversight framework, particularly that of data protection authorities (DPAs), to monitor, investigate, and intervene effectively in increasingly complex and opaque data infrastructures. As central components of the GDPR's integrated oversight framework, DPAs play a key role in monitoring and enforcement. They are also responsible for shaping data protection norms, facilitating dialogue with stakeholders and supporting compliance through awareness-raising and guidance (Jori 2015; Raab and Szekely 2017). However, many countries still lack a specialized and independent supervisory authority for data protection (Gao 2021; Widiatedja and Mishra 2023). Where such authorities exist, limited resources and powers often constrain their ability to respond effectively to the complex and systemic risks posed by large-scale data processing and new technologies such as AI (Raab and Szekely 2017).

It is therefore essential that a specialised data protection authority is in place, with sufficient independence, resources and technological expertise to represent the public interest in the governance of data infrastructures (Jori 2015; Schütz 2022). It is also important to grant the supervisory authority sufficient *ex ante* investigatory competence and *ex post* punitive power. For instance, they should be able to conduct black box testing proactively to detect manipulative and socially harmful data processing. They should also be able to require regulated entities to provide both technical and non-

technical information necessary for effective oversight, including information about model weights, training data, techniques, and relevant parameters used in the development of machine-learning systems. They should also have the power to impose sanctions on organisations and, where appropriate, responsible executives, and to order the reorganisation of data-driven systems where structural failures or systemic non-compliance are identified (Cohen et al. 2024). These powers are necessary to ensure that complex data infrastructures remain contestable and correctable in the public interest.

Yet stronger supervisory authorities alone are insufficient. Recognising the ethical and infrastructural dimensions of data protection also highlights the need for participatory governance mechanisms that enable broader public engagement in overseeing data-driven systems. Collective enforcement mechanisms, such as group actions for injunctions or compensation, should be a standard rather than an optional component of data protection regimes, particularly in cases involving dispersed or non-material harm (Sartor and Lagioia 2020; Linden and Walree 2018). Reconceptualising data protection as infrastructure regulation also requires that such mechanisms be directed toward detecting and correcting systemic risks rather than merely aggregating individual grievances. This, in turn, entails empowering not-for-profit bodies and other qualified organisations with the expertise and independence to act without individual mandates, enabling them to identify patterns of non-compliance and represent societal rather than individual interests (Golunova and Eliantonio 2024). Democratising oversight can also be advanced by institutionalising the collective exercise of data subject rights, for example by allowing specialised Data Rights Intermediaries (DRIs) to coordinate and exercise inalienable rights on behalf of data subjects at scale (Giannopoulou et al. 2022). In this way, these organisations can function as durable mechanisms for detecting systemic risks and collective harms within the broader oversight architecture.

In infrastructural settings, effective oversight depends not only on formal enforcement powers but also on distributed capacities to generate knowledge about how systems operate and whom they affect. While the GDPR already provides a partial foundation for such oversight, Cohen et al. (2024) propose several additional forms of participatory oversight. These mechanisms include community-led research, participatory audits, and public advocacy. They would enable affected communities, local organisations, journalists, researchers, and workers to participate directly in the monitoring and governance of data infrastructures. Such bottom-up practices complement state-centred forms of oversight and play an important role in enhancing the legitimacy and public trustworthiness of data infrastructures. Cohen et al. also suggest establishing a “Public Research Institute” to develop procedures for, and administer access requests from members of the public, who require information on data-driven systems and the entities controlling them in order to study their societal impact (p 18). Such an institute could facilitate broader and more diverse forms of expert scrutiny, support supervisory

authorities, and help reduce information and power asymmetries between technology companies and the public.

7. Conclusion

Building on recent scholarship conceptualising data as infrastructure, this article has argued that data protection law is best understood as a form of infrastructure regulatory regime rather than an extension of the right to privacy. Recognising and correcting the ethical misdiagnosis between data protection and privacy is not just an academic refinement. Only when the broader ethical and social values implicated by the processing of personal data are widely acknowledged can legislatures meaningfully adapt existing legal frameworks and adopt targeted measures to effectively address the challenges posed by data-driven systems. In support of this reconceptualisation, the article has proposed three key policy directions: reframing the prevailing narrative that portrays data protection as a trade-off for innovation; shifting the emphasis from individual control to institutional accountability; strengthening independent oversight authorities and fostering participatory public monitoring mechanisms. These reforms would allow data protection law to address more effectively the societal problems and systemic risks posed by the automated processing of personal data, by ensuring that data infrastructures are governed in a manner that promotes institutional accountability, supports public monitoring and advances broader ethical values, rather than relying solely on individual rights.

Data availability

Data sharing is not applicable to this research as no data were generated or analysed.

Competing interests

The authors declare no competing interests.

Ethical approval

The study does not involve human participants or their data and therefore does not require ethical approval. It is a doctrinal and policy analysis based on published academic work, legislation, cases and news reports.

Informed consent

Not applicable because the study does not involve human participants.

References

Altman I (1977) Privacy regulation: culturally universal or culturally specific? Journal of Social Issues 33:66–84

Andrejevic M (2007) Surveillance in the digital enclosure. Communication Review 10:295–317

Andrejevic M (2008) Privacy, exploitation, and the digital enclosure. Amsterdam Law Forum 1(4):47–62

Article 29 Data Protection Working Party (WP29) (2011) Advice paper on special categories of data ("sensitive data"). https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf. Accessed 20 May 2025

Balkin JM (2020) The fiduciary model of privacy. Harvard Law Review Forum 134:11–33

Bennett CJ (1992) Regulating privacy: data protection and public policy in Europe and the United States. Cornell University Press, Ithaca and London

Bergkamp L (2002) EU data protection policy: the privacy fallacy: adverse effects of Europe's data protection policy in an information-driven economy. Computer Law & Security Review 18(1):31–47

Bietti E (2025) Data is infrastructure. Theoretical Inquiries in Law 26:55–87. https://ssrn.com/abstract=5041965. Accessed 20 May 2025

Birnhack MD (2008) The EU Data Protection Directive: an engine of a global regime. Computer Law & Security Review 24:508–520

Borak M (2021) China's privacy law borrows a page from Europe's GDPR but it goes further as Beijing shores up data security. South China Morning Post. https://www.scmp.com/tech/tech-war/article/3146523/chinas-privacy-law-borrows-page-europes-gdpr-it-goes-further-beijing. Accessed 20 May 2025

Bundesverfassungsgericht (1983) Census Judgment, BVerfGE 65, 1, 1 BvR 209, 269, 362, 420, 440, 484/83, 15 December 1983. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html. Accessed 20 May 2025

Burkert H (2009) Towards a new generation of data protection legislation. In: Gutwirth S, Poullet Y, De Hert P, de Terwangne C, Nouwt S (eds) Reinventing data protection? Springer, Dordrecht, pp 335–342

Bygrave LA (1998) Data protection pursuant to the right to privacy in human rights treaties. International Journal of Law and Information Technology 6(3):247–284

Bygrave LA (2001) The place of privacy in data protection law. University of New South Wales Law Journal 24:277–282

Bygrave LA (2002) Data protection law: approaching its rationale, logic and limits. Kluwer Law International, The Hague/New York

Capurro R (2005) Privacy: an intercultural perspective. Ethics and Information Technology 7:37–47

Case C-369/98 (2000), The Queen v Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher, Opinion of Advocate General Alber, ECLI:EU:C:2000:79, 10 February 2000

Chander A, Kaminski ME, McGeveran W (2021) Catalyzing privacy law. Minnesota Law Review 105:1733–1801

Chander A, Schwartz P (2023) Privacy and/or trade. University of Chicago Law Review 90:49–135

Cinelli M, De Francisci Morales G, Galeazzi A, Quattrociocchi W, Starnini M (2021) The echo chamber effect on social media. Proceedings of the National Academy of Sciences of the United States of America 118(9):1–8

Citron DK (2010) Mainstreaming privacy torts. California Law Review 98:1805–1852

Cockcroft S, Rekker S (2016) The relationship between culture and information privacy policy. Electronic Markets 26:55–72

Cohen JE (2013) What privacy is for. Harvard Law Review 126:1904–1933

Cohen JE (2019) Between truth and power: the legal constructions of informational capitalism. Oxford University Press, New York

Cohen JE (2024) Platforms, data infrastructures, and infrastructure stacks. Georgetown University Law Center Research Paper No. 2023/25. Forthcoming in Johns F, Sullivan G, Van Den Meerssche D (eds) Global governance by data: infrastructures of algorithmic rule. Cambridge University Press. https://ssrn.com/abstract=4693056. Accessed 20 May 2025

Cohen JE, Ohm P, Jones ML, Dvoskin B, Krishna Prasad S (2024) Regulatory monitoring in the information economy. Washington University in St. Louis Legal Studies Research Paper. https://ssrn.com/abstract=4958179. Accessed 20 May 2025

Council of Europe (1973) Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted 26 September 1973, Strasbourg

Council of Europe (1974) Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, adopted 20 September 1974, Strasbourg

Council of Europe (1981) Convention for the protection of individuals with regard to automatic processing of personal data, ETS No. 108, opened for signature 28 January 1981, Strasbourg

Dalla Corte L (2020) A right to a rule: on the substance and essence of the fundamental right to personal data protection. In: Hallinan D, Leenes R, Gutwirth S, De Hert P (eds) Data protection and privacy: data protection and democracy. Hart Publishing, Oxford, pp 27–58

De Hert P, Gutwirth S (2006) Privacy, data protection and law enforcement: opacity of the individual and transparency of power. In: Claes E, Duff A, Gutwirth S (eds) Privacy and the criminal law. Intersentia, Antwerp/Oxford, pp 61–104

De Hert P, Gutwirth S (2009) Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: Gutwirth S, Poullet Y, De Hert P, de Terwangne C, Nouwt S (eds) Reinventing data protection? Springer, Dordrecht, pp 3–44

Diggelmann O, Cleis MN (2014) How the right to privacy became a human right. Human Rights Law Review 14(3):441–458

Dodds L, Wells P (2019) Data infrastructure. In: Davies T, Walker SB, Rubinstein M, Perini F (eds) The state of open data: histories and horizons. African Minds and International Development Research Centre, Cape Town and Ottawa, pp 260–273

Ess C (2005) 'Lost in translation'? intercultural dialogues on privacy and information ethics. Ethics and Information Technology 7(1):1–6

European Commission (2020) Communication from the Commission to the European Parliament and the Council: 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. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0264. Accessed 5 November 2025

European Commission (2024) Communication from the Commission to the European Parliament and the Council: second report on the application of the General Data Protection Regulation, COM(2024) 357 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024DC0357. Accessed 5 November 2025

European Commission (2025) Omnibus IV simplification package. https://single-market-economy.ec.europa.eu/publications/omnibus-iv_en. Accessed 5 November 2025

European Union Agency for Fundamental Rights (FRA) (2024) GDPR in practice: experiences of data protection authorities. https://fra.europa.eu/en/publication/2024/gdpr-experiences-data-protection-authorities. Accessed 20 May 2025

Frischmann BM (2012) Infrastructure: the social value of shared resources. Oxford University Press, New York

Fuster GG (2014) The emergence of personal data protection as a fundamental right of the EU. Springer, Cham

Fuster GG, Gutwirth S (2013) Opening up personal data protection: a conceptual controversy. Computer Law & Security Review 29:531–539

Future of Privacy Forum (2021) From 'consent-centric' frameworks to responsible data practices and privacy accountability in Asia Pacific. https://fpf.org/blog/event-report-from-consent-centric-frameworks-to-responsible-data-practices-and-privacy-accountability-in-asia-pacific. Accessed 20 May 2025

Gal MS, Aviv O (2020) The competitive effects of the GDPR. Journal of Competition Law & Economics 16(3):349–391

Gao K (2021) On the establishment of a specialized agency for personal information protection. Law Review 39(6):106–118

Gellert R, Gutwirth S (2013) The legal construction of privacy and data protection. Computer Law & Security Review 29(5):522–530

Giannopoulou A, Ausloos J, Delacroix S, Janssen H (2022) Intermediating data rights exercises: the role of legal mandates. International Data Privacy Law 12(4):316–331

Glancy DJ (1979) The invention of the right to privacy. Arizona Law Review 21:1–28

Global Infrastructure Hub (2021) Connectivity across borders: global practices for cross-border infrastructure projects. https://www.gihub.org/connectivity-across-borders. Accessed 5 November 2025

Goldman E (2023) Privacy law is devouring internet law (and other doctrines) … to everyone's detriment. Technology & Marketing Law Blog, 9 May. https://blog.ericgoldman.org/archives/2023/05/privacy-law-is-devouring-internet-law-and-other-doctrines-to-everyones-detriment.htm. Accessed 20 May 2025

Golunova V, Eliantonio M (2024) Civil society actors as enforcers of the GDPR: what role for the CJEU? Journal of Intellectual Property, Information Technology and Electronic Commerce Law 15:180–193

Graef I, van der Sloot B (2022) Collective data harms at the crossroads of data protection and competition law: moving beyond individual empowerment. European Business Law Review 33:513–536

Greenleaf G (2014) Asian data privacy laws: trade and human rights perspectives. Oxford University Press, Oxford

Greenleaf G (2015) Hong Kong data privacy 2015: cautious enforcement, strong principles. Privacy Laws & Business International Report 138:21–23

Griswold v Connecticut, 381 U.S. 479 (1965)

Guo Z (2025) Criminalisation of the illegal use of personal data: comparative approaches and the Chinese choice. Humanities and Social Sciences Communications 12:782

Han XZ (2021) Geren xinxi baohu zhong gaozhi tongyi de kunjing yu chulu: jianlun geren xinxi baohu fa caoan xiangguan tiaokuan (Difficulties of notice and consent in personal information protection and solutions: with a focus on the relevant provisions of the Chinese Personal Information Protection Law). Economic and Trade Law Review 1:47–58

Hartzog W (2021) What is privacy? That's the wrong question. University of Chicago Law Review 88(7):1677–1688

Hartzog W, Richards NM (2020) Privacy's constitutional moment and the limits of data protection. Boston College Law Review 61:1687–1761

Hondius FW (1975) Emerging data protection in Europe. North-Holland Publishing, Amsterdam

Hondius FW (1980) Data law in Europe. Stanford Journal of International Law 16:87–111

Hornung G, Schnabel C (2009) Data protection in Germany I: the population census decision and the right to informational self-determination. Computer Law & Security Review 25(1):84–88

Humphrey JP (1984) Human rights and the United Nations: a great adventure. Transnational Publishers, Dobbs Ferry, NY

Hustinx P (2014) European leadership in privacy and data protection. European Data Protection Supervisor. https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/european-leadership-privacy-and-data_en. Accessed 20 May 2025

Igaya S, Sudoh O (2025) Ignored discrepancies in the fundamental concepts of data protection laws in Japan and the EU. International Data Privacy Law 15(2):171–186

International Association of Privacy Professionals (2025) Reforming the GDPR for tomorrow's technologies: why Europe needs targeted GDPR reform. https://iapp.org/news/a/reforming-the-gdpr-for-tomorrow-s-technologies-why-europe-needs-targeted-gdpr-reform. Accessed 5 November 2025

Janofsky A (2019) One year into GDPR, companies prepare for more privacy regulations. The Wall Street Journal. https://www.wsj.com/articles/one-year-into-gdpr-companies-prepare-for-more-privacy-regulations-11557955595. Accessed 20 May 2025

Jori A (2015) Shaping vs applying data protection law: two core functions of data protection authorities. International Data Privacy Law 5(2):133–143

Katz v United States, 389 U.S. 347 (1967)

Kitiyadisai K (2005) Privacy rights and protection: foreign values in the modern Thai context. Ethics and Information Technology 7:17–26

Kokott J, Sobotta C (2013) The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law 3(4):222–228

Kramer IR (1989) The birth of privacy law: a century since Warren and Brandeis. Catholic University Law Review 39:703–724

Krotoszynski RK Jr (2016) Privacy revisited: a global perspective on the right to be left alone. Oxford University Press, New York

Lapowsky I (2019) How Cambridge Analytica sparked the great privacy awakening. WIRED. https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening. Accessed 20 May 2025

Linden TE van der, Walree TF (2018) De collectieve procedure als oplossing voor het privaatrechtelijke handhavingstekort bij een datalek? (The collective procedure as a

remedy for the private-law enforcement deficit in data-breach cases). Liability, Insurance and Damage 19(4):105–113

Lynskey O (2012) From market-making tool to fundamental right: the role of the Court of Justice in data protection's identity crisis. In: Gutwirth S, Leenes R, De Hert P, Poullet Y (eds) European data protection: coming of age. Springer, Dordrecht, pp 59–84

Lynskey O (2014) Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order. International and Comparative Law Quarterly 63(3):569–597

Lynskey O (2015) The foundations of EU data protection law. Oxford University Press, Oxford

Lyon D (ed) (2003) Surveillance as social sorting: privacy, risk, and digital discrimination. Routledge, London

Lyon D (2010) Surveillance, power and everyday life. In: Kalantzis-Cope P, Gherab-Martín K (eds) Emerging digital spaces in contemporary society. Palgrave Macmillan, London, pp 107–120

Lyon D (2019) Surveillance capitalism, surveillance culture and data politics. In: Bigo D, Isin E, Ruppert E (eds) Data politics: worlds, subjects, rights. Routledge, Abingdon and New York, pp 64–77

Mahieu R (2021) The right of access to personal data: a genealogy. Technology and Regulation 2021:62–65

Mantelero A (2018) AI and big data: a blueprint for a human rights, social and ethical impact assessment. Computer Law & Security Review 34(4):754–772

Matzner T, Mann M (2019) Challenging algorithmic profiling: the limits of data protection and anti-discrimination in responding to emergent discrimination. Big Data & Society 6(2):1–15

McQuinn A, Castro D (2019) The costs of an unnecessarily stringent federal data privacy law. Information Technology and Innovation Foundation. https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law. Accessed 20 May 2025

Miller Miller et al. (2016) How the world changed social media. UCL Press, London

Mostert M et al (2018) From privacy to data protection in the EU: implications for big data health research. European Journal of Health Law 25:43–51

Nakada M, Tamura T (2005) Japanese conceptions of privacy: an intercultural perspective. Ethics and Information Technology 7:27–30

Niebel C (2021) The impact of the General Data Protection Regulation on innovation and the global political economy. Computer Law & Security Review 40:105523

Nissenbaum H (2009) Privacy in context: technology, policy, and the integrity of social life. Stanford University Press, Stanford, CA

Olmstead v United States, 277 U.S. 438 (1928)

Open Data Institute (2023) Global data infrastructure. https://theodi.org/insights/projects/global-data-infrastructure. Accessed 3 November 2025

Post R (2017) Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. Duke Law Journal 67:981–1072

Prins C (2006) Property and privacy: European perspectives and the commodification of our identity. In: Guibault L, Hugenholtz PB (eds) The future of the public domain: identifying the commons in information law. Kluwer Law International, The Netherlands, pp 223–257

Prosser WL (1960) Privacy. California Law Review 48:383–423

Purtova N, Newell BC (2025) Against data fixation: why 'data' fails as a regulatory target for data protection law and what to do about it. Oxford Journal of Legal Studies, in press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4878564. Accessed 3 November 2025

Raab C, Szekely I (2017) Data protection authorities and information technology. Computer Law & Security Review 33(4):421–433

Rauhofer J (2014) Round and round the garden? Big data, small government and the balance of power in the information age. Edinburgh School of Law Research Paper 2014/6:1–12

Regan PM (1995) Legislating privacy: technology, social values, and public policy. University of North Carolina Press, Chapel Hill, NC

Richards N, Hartzog W (2020) A relational turn for data protection? European Data Protection Law Review 4:492–497

Rodotà S (2009) Data protection as a fundamental right. In: Gutwirth S, Poullet Y, De Hert P, de Terwangne C, Nouwt S (eds) Reinventing data protection? Springer, Dordrecht, pp 77–82

Rubinstein IS, Good N (2020) The trouble with Article 25 (and how to fix it): the future of data protection by design and default. International Data Privacy Law 10(1):37–56

Sartor G, Lagioia F (2020) The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530. Accessed 20 May 2025

Schütz P (2022) Data protection authorities under the EU General Data Protection Regulation: a new global benchmark. In: Maggetti M, Di Mascio F, Natalini A (eds) Handbook of regulatory authorities. Edward Elgar Publishing, Cheltenham and Northampton, MA, pp 128–145

Schwartz P (1989) The computer in German and American constitutional law: towards an American right of informational self-determination. The American Journal of Comparative Law 37(4):675–701

Schwartz PM (2019) Global data privacy: the EU way. New York University Law Review 94:771–818

Segerstedt-Wiberg v Sweden, App no 62332/00, European Court of Human Rights, 6 June 2006

Shao G et al (2025) Assessing the implementation of China's personal information protection law: a two-year review. International Data Privacy Law 15:18–31

Shen J (2019) Chengfaxing jianguan youai chuangxin yu chengzhang: cong ouzhou GDPR tanqi (Punitive regulation hampers innovation and growth: lessons from Europe's GDPR). Jingdong Digital Technology Research Institute. https://www.secrss.com/articles/14378. Accessed 20 May 2025

Simitis S (1987) Reviewing privacy in an information society. University of Pennsylvania Law Review 135(3):707–746

Solove DJ (2001) Privacy and power: computer databases and metaphors for information privacy. Stanford Law Review 53:1393–1462

Solove DJ (2002a) Conceptualizing privacy. California Law Review 90:1087–1155

Solove DJ (2002b) Identity theft, privacy, and the architecture of vulnerability. Hastings Law Journal 54:1227–1276

Solove DJ (2004) The digital person: technology and privacy in the information age. New York University Press, New York and London

Solove DJ (2005) A taxonomy of privacy. University of Pennsylvania Law Review 154:477–564

Solove DJ (2023) The limitations of privacy rights. Notre Dame Law Review 98:975–1036

Spohr D (2017) Fake news and ideological polarization: filter bubbles and selective exposure on social media. Business Information Review 34(3):150–160

Stoddart E (2014) (In)visibility before privacy: a theological ethics of surveillance as social sorting. Studies in Christian Ethics 27:33–49

Sun Q (2022) Guojia jiguan chuli geren xinxi de teshu fengxian jiqi falü guizhi (Special risks and legal regulations of government agencies dealing with personal information). Journal of Anhui University (Philosophy and Social Science Edition) 3:88–92

Tuch AF (2020) A general defense of information fiduciaries. Washington University Law Review 98:1897–1937

Tzanou M (2017) The fundamental right to data protection: normative value in the context of counter-terrorism surveillance. Hart Publishing, Oxford

Van Ooijen I, Vrabec HU (2019) Does the GDPR enhance consumers' control over personal data? An analysis from a behavioural perspective. Journal of Consumer Policy 42:91–107

Van den Hoven J (2008) Information technology, privacy, and the protection of personal data. In: Van den Hoven J, Weckert J (eds) Information technology and moral philosophy. Cambridge University Press, Cambridge, pp 301–321

Viljoen S (2024) The broader lessons of privacy law. Boston University Law Review 104(4):1131–1150

Wacks R (2015) Privacy: a very short introduction. Oxford University Press, Oxford

Waldman AE (2021) The new privacy law. UC Davis Law Review Online 55:19–42

Wang X, Peng C (2021) Geren xinxi baohu falü tixi de xianfa jichu (On the constitutional basis of the personal information protection regime). Tsinghua University Law Journal 15(3):6–24

Warren SD, Brandeis LD (1890) The right to privacy. Harvard Law Review 4(5):193–220

Westin AF (1967) Privacy and freedom. Atheneum, New York

Widiatedja IGNGP, Mishra N (2023) Establishing an independent data protection authority in Indonesia: a future-forward perspective. International Review of Law, Computers & Technology 37(3):252–273

Yadav AK, Suryadevara S (2023) Advances in data protection and artificial intelligence: trends and challenges. International Journal of Advanced Engineering Technologies and Innovations 1(1):294–319

Yang L, Yan M (2021) The conceptual barrier to comparative study and international harmonisation of data protection law. Hong Kong Law Journal 51:917–941

Yeung K (2016) Hypernudge: big data as a mode of regulation by design. Information, Communication & Society 20:118–136

Yeung K (2018) Five fears about mass predictive personalization in an age of surveillance capitalism. International Data Privacy Law 8(3):258–269

Yeung K, Bygrave LA (2022) Demystifying the modernized European data protection regime: cross-disciplinary insights from legal and regulatory governance scholarship. Regulation & Governance 16(1):137–142

Zhang J (2021) Geren xinxi heli shiyong de lifa chuangxin yu caipan lichang (Legislative innovation and judicial stance on the reasonable use of personal information). Seeking Truth Journal 6:112–120

Zhou H (2021) Pingxing haishi jiaocha: geren xinxi baohu yu yinsi quan de guanxi (Parallelism or intersection: on the relationship between personal information protection and the right to privacy). Peking University Law Journal 5:1167–1187

Zuboff S (2016) The secrets of surveillance capitalism. Frankfurter Allgemeine Zeitung, 5 March. https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html. Accessed 20 May 2025

Zuboff S (2019a) Surveillance capitalism and the challenge of collective action. New Labor Forum 28(1):10–25

Zuboff S (2019b) The age of surveillance capitalism: the fight for a human future at the new frontier of power. Profile Books, London

Endnotes

[1] For example, the United States' Privacy Act of 1974, Australia's Privacy Act of 1988, Hong Kong's Personal Data (Privacy) Ordinance of 1995 and Philippines Data Privacy Act of 2012.

[2] Although the right to privacy is commonly traced to Warren and Brandeis's 1890 formulation, the Indian case Gokal Prasad v. Radho (1888), decided by a British colonial court, is occasionally cited as an earlier recognition. However, it neither established the conceptual foundation nor exerted the lasting influence that Warren and Brandeis's work would later achieve.

[3] To be precise, when the Directive was adopted in the 1990s, its main legal basis and policy focus lay in promoting the free flow of personal data between member states to facilitate market integration. This reflected the European Community's limited legislative competence under the pre-Lisbon Treaty framework, whereby measures had to be justified as contributing to market integration under the Community pillar. It was only after the Treaty of Lisbon made the EU Charter of Fundamental Rights legally binding in 2009 that the protection of fundamental rights became an equally important objective alongside market harmonisation (Lynskey 2012; Lynskey 2015, pp 61–62).

[4] However, unlike the Directive, the emphasis on the right to privacy has been removed from the GDPR's article on objectives (Article 1).

[5] Shoshana Zuboff also refers to it as "behaviour modification" (Zuboff 2019, p 8).

[6] For example, in Ling v Douyin (2020), a high-profile Chinese case involving Douyin, the Chinese version of TikTok, the Beijing Internet Court acknowledged that the information collected by Douyin (i.e., the names and mobile phone numbers of users' contacts) constituted personal data, and that Douyin had failed to obtain the data subjects' consent as required by law. Nevertheless, the court held that Douyin's data collection constituted a reasonable use of personal data and was therefore not unlawful. In its reasoning, the court emphasised that "data is an important production factor in the era of the digital economy," and that "overly absolute protection of personal data" could impose excessive costs on data use, thereby hindering the development of the information industry and society at large (at pp 40–43). See Zhang (2021) for further discussion.

Ethics Statements

The study does not involve human participants or their data and therefore does not require ethical approval and informed consent.