



Beyond Notice and Consent: A Jurisprudential Evaluation of the Europe's GDPR and India's DPDP Act in an AI-DRIVEN Ecosystem

*Vanshika Jain¹, A.P. Bhanu², Aayushi Goel³

¹ Junior Research Fellow, Symbiosis International University, Pune, India

² Professor- Law, Researcher and Addl. Director, Amity Law School, Amity University, Noida, India and Adjunct professor of Law at ALS, University of Adelaide, Australia

³ Assistant Professor, Symbiosis Law School, Noida, India
vanshikajain423@gmail.com

Abstract. Human life has become increasingly influenced by algorithms, automated decision-making systems, and extensive data analytics, creating a digital environment in which individuals are continuously monitored, profiled, and evaluated. Although legislatures worldwide have responded to this pervasive surveillance infrastructure by introducing privacy and data governance frameworks grounded in ethical principles such as transparency, accountability, and fairness. However, their approaches remain largely based on Alan Westin's Notice-and-Consent model, which is only reactive and is insufficient to address the deeper challenges posed by AI-based technology, especially to digital autonomy, which is threatened due to the continuous storage, processing, and utilization of individual data without meaningful consent. Therefore, this paper argues that the contemporary data governance regimes must move beyond mere procedural compliance and be 're-constructed' on the philosophical and normative foundations of privacy. Adopting a Doctrinal, comparative, and Normative methodology, the paper compares Europe's GDPR, which was adopted in 2016, with India's DPDP Act adopted in 2023. The focus on these laws is based on the time gap between their adoption, during which AI-based technology became more deeply integrated into society. This allows the paper to examine whether the laws reflect this technological shift and incorporate more advanced or evolved understandings of privacy. Drawing on the works of Warren and Brandeis, Alan Westin, Judith Jarvis Thompson, and Helen Nissenbaum, along with the critical philosophers of privacy, the paper assesses the evolution of understanding of individual privacy to its contextual and relational understandings. The paper further uses Kantian and Rawlsian perspectives of justice and fairness to evaluate GDPR & DPDP. In doing so, the paper argues for a value-centric model of digital governance that embeds autonomy and human dignity into the design of the regulatory framework thereby enabling an anticipatory and grounded approach to privacy regulation worldwide.

Keywords: Privacy, Digital Autonomy, Data Governance, Philosophies of Privacy

1 Introduction

With the rise in digital infrastructure and a technology-dependent society, data has become a ‘resource’ to analyze and predict human behavior, and a means of governance, rather than just being a byproduct of human interaction. (Birch et al., 2021). We are surrounded with technology and automated systems in more ways than we think; from target marketing that uses behavioral patterns to using automated systems and algorithms for critical decision-making such as assessing credit scores for loans, declaring fit for social welfare programs, daily surveillance by private institutions or government organizations, to assessing a criminal’s ability for committing a crime again. All of which is possible because of the digital footprints we leave on the internet, and the data these technologies collect and utilize. It is much like people have acquiesced to living in a ‘datafied’ society where, every human action is converted into quantifiable data and instead of an individual, their digital footprints account for them and their data is the prime asset. (Mayer-Schönberger & Cukier (2013). As a consequence, we have a ubiquitous surveillance infrastructure that quietly operates in the background of our digital lives, monitoring our behavior, influencing our choices, and selecting the data we consume. (Nishnianidze, 2024) “While on the one hand we often provide our personal information willingly in exchange for receiving access to these new technologies, on the other hand, the fine print disguised in the existing laws enables governments and giant technology conglomerates, often without bothering to ask for our consent, to amass vast amounts of personal information on large populations” (Moore et al., 2020).

In response to the risks posed by large-scale data collection and AI-driven decision making, legislatures, and international organizations have created regulatory frameworks to protect data privacy and cybersecurity. Privacy guidelines in the form of international standards and recommendations for legislatures across the globe have been provided by the OECD and the United Nations while regional and National legal frameworks in response to Moral and ethical dilemmas on privacy have also emerged. Among these, the European Union's General Data Protection regulation (GDPR), enacted in the year 2018, established the benchmark for comprehensive data protection legislation and has significantly influenced subsequent privacy laws worldwide including India's Data Privacy Regulation namely, The Digital personal Data Privacy Act (DPDP). However, DPDP act was enacted in the year 2023 nearly after five years, at the cusp of rapid emergence of generative AI and advanced algorithmic systems, after AI had fundamentally transformed the collection, processing, and use of personal data. The temporal gap between these two legislative frameworks provides an important opportunity to examine whether the evolution of privacy legislation has been accompanied by a corresponding evolution of normative understanding of privacy required for regulation of privacy in the AI-driven ecosystem.

Both of these legislations operationalize privacy predominantly using Westin's Notice and consent model only, thereby reducing a rich philosophical inheritance of Privacy to a mere procedural checkbox. While consent remains an important safeguard, increasing reliance on opaque AI systems, automated decision-making, behavioral predictions and algorithmic profiling raises important questions regarding whether consent alone remains sufficient to protect individual 'autonomy' and ensure 'fairness' in contemporary data governance. Therefore, the central challenge confronting privacy regulation is no longer merely of the collection/ processing of personal information, but whether existing legal frameworks adequately respond to the ethical and distributive challenges created by AI-driven societies.

To address the gaps in the regulatory frameworks of these nations, this paper traces the philosophical underpinnings of privacy and cybersecurity through a full arc of classical and modern legal and ethical theories on privacy starting from Warren & Brandies foundational right “to be left alone” in 18th century (The Right to Privacy in Nineteenth Century America, 1981), Alan Westin’s self-determination model (Westin, 1968), Thomson’s Pluralist View on privacy in the late 19th century (Thomson, 1975), and Helen Nissenbaum’s theory of “contextual integrity” (Nissenbaum, 2009). These foundational theories are further complemented by communitarian views of Taylor and the critical perspective of Foucault and Zuboff on surveillance, power and digital surveillance.

Building upon this jurisprudential evolution, the paper adopts the Kantian tradition, which emphasizes human dignity and rational agency (Rohlf, 2022), and the Rawlsian framework of justice as fairness which stipulates that the monarch (government) has a responsibility to establish systems in a way that is under the apprehension that people are unaware of their own social position (Wenar, 2021) to evaluate whether contemporary privacy laws adequately protect digital autonomy and distributive justice in the present generation of Artificial Intelligence. Instead of seeing these theories as competing alternatives, this paper theorizes them as complementary stages in the evolution of privacy jurisprudence. Seen together, these theories demonstrate that protecting privacy extends beyond mere procedures of notice and consent and includes Autonomy, dignity, contextual integrity, distributive fairness, and meaningful limitations on surveillance infrastructure around us. These normative principles constitute the evaluative framework through which the GDPR and DPDP act are analyzed.

1.1 Review of Literature

Privacy has evolved from just a concept to the most asked human right in the present times. The evolution of privacy from being a part of theories of early jurists to being a part of legislative debates is largely technologically driven.

Most regulatory frameworks today have adopted Westin’s notice and consent framework to protect individual privacy; however, as rightly pointed out by (Orrù, 2021), these liberal-individualist notions have been proven insufficient in today’s digital environments, where data is routinely collected and the concept of control is frequently illusory. His review of normative and skeptical methods questions the underlying assumptions that support existing laws.

(Stalder, 2002) critique of “informational self-determination” as a protective “bubble” contends that individualistic control-over-entry metaphors are out of place in

a networked environment where data flows, inference, and aggregation go beyond any one individual's control. These criticisms collectively explain why frameworks that depend on individual control and a rigid distinction between the public and private sectors fail in modern data ecosystems.

(Helm & Seubert, 2020) contend that “privacy literacy” and “choice” in platform capitalism are riddled with normative contradictions. Even ‘literate’ consumers are unable to exercise their autonomy when market structures, and architectures are designed in a way that encourages one to share or disclose their information and rejecting such disclosure is made either expensive or limits access. As a result, there is a predictable gap between actual authority given to the consumers and official capacity to consent to the disclosure of information.

ByGrave (2014) argues that data privacy constitutes a lucid legal discipline founded upon the protection of broader values such as autonomy, dignity, and democratic participation, instead of simply detailing procedural obligations for data controllers. Similarly, Kuner (2020) characterizes the GDPR as the ‘contemporary’ global benchmark for privacy governance whose influence extends beyond Europe and has shaped subsequent privacy legislation across jurisdictions, including India’s Digital Personal Data Privacy Act, 2023. This body of scholarship suggests that modern privacy legislation should be evaluated not only for its regulatory effectiveness but also for the philosophical conception it embodies.

Despite their significance, these laws are not enough to address the fundamental power disparities in present day ‘datafied’ society. These literary notice and consent systems may even result in “normative paradoxes”, which legitimize exploitative practices by presenting them as options, thereby increasing rather than decreasing individual vulnerability. (Helm & Seubert, 2020). Similarly, (Knijnenburg et al., 2022) says that contemporary society’s privacy concerns are social, technical, and collective, affecting healthcare systems, linked devices, and vulnerable communities, but regulatory frameworks continue to treat privacy as an individual benefit. In general, Allen (2013) distinguishes between normative theories, which assess laws against ethical criteria, and positive theories of privacy law, which identify the winners and losers of current regulations.

More recently, the present privacy law of India i.e. the DPDP Act, 2023, has also begun to move beyond purely doctrinal analysis towards jurisprudential enquiry questioning whether the act represents the genuinely right-based conception of privacy or continues the procedural logic inherited from earlier consent-based conception of privacy models (Jadhao, 2026)

The available literature is focused on a key contradiction: privacy is theoretically and normatively connected to autonomy, dignity, and democratic involvement, but regulatory practice continues to operationalize it in constrained, procedural terms. This disconnection accounts for the persistence of harm such as profiling, discrimination, illegal data extraction, and manipulative design (Kathuria et al., 2024; Ding & Huang, 2024). While existing scholarship has extensively critiques the limitations of Notice and consent Mechanism (Jordan, 2021), comparatively less attention has been devoted to examine whether the legislative evolution from GDPR (2016) to DPDP (2023) across a period of marked by transformative rise of AI has been accompanied by a corresponding evolution in the normative understanding of privacy. Without reorientation of the current privacy regime, Privacy risks will continue to be reduced to a

regulatory checkbox rather than being maintained as a fundamental moral and democratic imperative unless there is such a reorientation.

1.2 Statement of the Problem

In spite of the increase in regulations and principles regarding privacy, especially data privacy, privacy violations continue to exist and proliferate. Certain activities such as Profiling, discrimination, unauthorized data extraction, and manipulative digital environments as assessed by (Kathuria et al., 2024) continue to undermine human autonomy, which suggests a deep chasm between the normative objectives that current regulatory frameworks seek to safeguard in the present-day “Datafied” society. Presently, Artificial Tools have become very accessible, which has certainly exacerbated the privacy risks, making them increasingly structural, automated, and difficult to address using traditional regulatory mechanisms.

The present compliance-focused strategy of legislatures across the globe lacks a strong ethical basis. Existing frameworks largely take a procedural, compliance-driven approach to privacy that is centered around notice and consent, which is insufficient to address the fundamental power imbalances in modern, data-driven contexts. (Kisselburgh & Beever, 2022). This limitation is particularly evident in contemporary privacy regulation such as the European Union’s General Data Protection Regulation (2016), and India’s Digital personal Data Protection Act (2023). Although enacted at different stages in the evolution of digital technologies, both frameworks continue to operationalise privacy predominantly using Notice-and consent mechanism and whereas consent does constitute a major part in protecting privacy, it has failed to account for other normative principles of privacy that has evolved since the Westin’s self-determination model in the 19th century. These frameworks failed to view privacy as a normative commitment related to the fundamental values of a democratic and equitable society, and rather see it simply as a regulatory checkbox (Ding & Huang, 2024)

The study therefore focuses on the normative inadequacies of DPDP Act, 2023 in parallel to the emergence of Artificial tools and the influence of GDPR, 2016 in protecting individual autonomy, moral agency, and human dignity. Although existing scholarship has extensively examined either the doctrinal operation of privacy legislation or the philosophical foundations of privacy, comparatively little attention has been paid in examining whether the successive generations of privacy legislation reflect a corresponding jurisprudential evolution in response to the Artificial Intelligence. More specifically, limited research has explored whether the transition from the GDPR, 2016 to the DPDP Act 2023, enacted after the rapid rise of AI technologies represents a meaningful shift in the philosophical understandings of privacy, autonomy, and justice or merely reproduced earlier approaches under a new legislative framework.

The paper determines at evaluating GDPR and DPDP from the lens of Kantian Digital autonomy and Rawlsian justice and fairness, to study whether legislative evolution has been accompanied by a corresponding evolution in the jurisprudential foundation of privacy.

As a result, the paper intends to promote a broader academic and political movement in favor of “anticipatory governance”, a framework that seeks to establish systems that

are aligned with ethical principles from the outset in order to prevent technological risks rather than merely reacting to them after they materialize. (Parrilli, 2024)

1.3 Research Methodology

To develop an understanding of the jurisprudential theories of privacy and the philosophical basis of contemporary privacy governance, the study adopts a qualitative doctrinal, comparative, and normative research methodology to examine the philosophical foundations of the contemporary privacy regime. The doctrinal approach analyses the constitutional principles, international instruments such as UDHR and OECD privacy guidelines, statutory frameworks, judicial developments, and scholarly literature while the normative approach evaluates if GDPR and DPDP adequately reflect the ethical values of autonomy, dignity, fairness and justice, principles that are adopted from other philosophies relating to privacy. The study employs a comparative legal analysis of General Data Protection regulation of the European Union, the Digital Personal Data Protection Act of India, through various privacy philosophies starting from Warren and Brandies to Zuboff & Foucault. The primal bases of such comparison shall be done using Kantian Digital Autonomy and Rawlsian Justice as Fairness.

2. Evolution of Privacy Jurisprudence

“Privacy is not simply a matter of what I can physically refuse to reveal about myself, but a matter of what I can refuse to reveal about myself”. (Garrett, 2005, para. 3)

The origin of privacy as a legal principle closely tracked shifts in societal organization, from intimate communities to increasingly networked and industrialized societies, where the public-private divide became increasingly porous. This jurisprudential evolution provides the foundation for evaluating whether contemporary privacy frameworks have evolved alongside technological transformations, particularly in light of development of the Artificial Intelligence based technology, and Data-driven governance.

The philosophical and legal conceptualization of privacy did not happen in a vacuum; rather, it evolved via a string of normative responses to societal and technological shifts. In the 19th century, when mass media and other contemporary technologies started to affect privacy, jurists and ethicists began to defend privacy as a legitimate right.

The very first attempt to define privacy as a ‘right’ was made by Warren and Louis Brandeis in 1890. They argued that the law needed to evolve to protect the “right to be let alone.” Their argument was prompted by the rise of technologies like mass journalism and instant photography, which threatened to breach the sanctity of private life. (Warren and Brandeis, 1890, p. 195) noted that “instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’” The statement by Warren and Brandeis was revolutionary in two key ways. “Firstly, identifying the harm, a right of privacy is predicated on mental anguish and feelings, that in and of themselves, were an actionable right to protect.” (Bycer, n.d.) Second, it redefined privacy as a vital part of one’s individuality and freedom. Warren and Brandeis argued that there must be

recognition of “privacy” as an individual right to provide any legal protection against actions that interfere with a person’s life. This helped lay the groundwork for subsequent privacy safeguards under constitutional and common law. It also helped establish the Right to Privacy under the UDHR and ICCPR. More significantly, Warren and Brandies’s work established privacy as a normative legal right that protects individual liberty and human dignity, thereby setting direction for subsequent jurisprudential developments on privacy.

Building upon the work of Warren & Brandies, the legal boundaries of privacy continued to be defined and redefined by scholars of the mid-19th century. A substantial contribution to define privacy in contemporary world was made by Alan Westin in 1967, through his book “Privacy and Freedom”, wherein he defined privacy as “claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others”, (Westin, 1967 p. 7) thereby emphasizing informational self-determination as both a moral right and a social policy goal. Furthermore, Westin also conceptualised different states of privacy i.e. (1) Solitude, (2) Intimacy, (3) Anonymity, (4) Reserve which according to (Marky, 2023) which collectively illustrate the different ways in which individuals exercise control over personal information in both physical and digital environments.

Amongst every privacy model that has sustained, the most influential and rather successful one is the notice-and-consent model, which, as per (Hoofnagle & Urban, 2014), was first proposed by Alan Westin in the form of segmentation of consumers into “privacy pragmatists,” “privacy fundamentalists,” and “privacy unconcerned”. The segmentation was suggested by Westin to study his peers and gain insights into their patterns as ‘consumer’ and their respective preferences. This notice and consent mechanism is fast adopted by legislatures today and has become a central model for data protection in privacy regulations across the globe particularly in GDPR, and subsequently, in the India’s DPDP Act as well. His notion encouraged policymakers and technologists to view privacy as a fundamental norm of democratic societies (that function on transparency) rather than just a transactional or technological concern. However, the model has also been criticized for its effectiveness in present day utilization of AI algorithms by organizations that function automatically and have ‘black box’ tendencies.

The pluralist view followed Westin’s work in the 1970s when Thomson made the case that privacy could not be defined by a single, comprehensive term (Varden, 2020) and contends that, “In addition to making many astute observations about how we commonsensically distinguish between various ethical and legal concerns with regard to respecting somebody’s privacy, Thomson argues that this lack of clarity exists, ultimately, because there is no such thing as one distinct right to privacy. Rather, she argues, what we subsume under the label of a “right to privacy” is a cluster of other rights central to liberty, most prominently the rights to bodily integrity and private property.” Her analysis represented a change in perspective from seeing privacy as a singular, separate right to seeing it as a derivative, relational, and contextual concept. This point of view serves as a ‘literary’ warning to the techno-Legal issues of licentious surveillance structures conducted by private as well as government organisations themselves (as seen in China), illustrating that privacy violations often include a broader constellation of rights rather than a single autonomous right to privacy.

The surveillance infrastructure also presents a stark resemblance to Big Brother’s omnipresent gaze in his fictional superstate in Oceania, symbolizing a world where even

one's thoughts and ideas are not safe. (Orwell, 1984). His work demonstrates the need of present-day privacy legislations to protect not only personal information but also individual autonomy, freedom of thought, and democratic participation in increasingly AI-driven societies.

Subsequently Critical and communitarian perspectives on privacy developed and reminded us that privacy is ultimately a social and political concept rather than simply a personal or an individual right. These perspectives offer an in-depth idea of the functionality of the right to privacy and how it is impacted by communities, institutions, and unequal power relationships. Given the communitarian perspective, the debate over privacy has been defined by theorists like Charles Taylor, Michael Sandel, and Alasdair MacIntyre in terms of what constitutes personal information, which then forms the three fundamental principles of the critical and communitarian perspective: (1) Character, (2) Narration, and (3) Tradition (Etzioni, 2000). When seen in silos, these perspectives challenge individualistic conceptions of privacy by situating personal information within a web of social, linguistic, and historical relations. (Moore, 2021) Further, the Charles Taylor's philosophical exposition, is not directly embedded in the concept of privacy but it propounds the concept of 'autonomy'. He views autonomy as inherently relational, not the atomistic freedom to choose, but the capacity to form one's identity through interaction with shared cultural and linguistic meanings. "When privacy and autonomy are connected, privacy is described as a way of controlling one's own personal environment. An invasion of privacy can also be seen as giving control over (or access to) one's personal sphere. This notion of privacy is closely related to secrecy" (Becker, 2019). Such a view of autonomy has direct implications for privacy in the digital age: when algorithmic systems pre-emptively curate choices, manipulate information exposure, or erode the individual's capacity to reflect and deliberate freely, they disrupt the very moral conditions that helps in sustaining 'autonomy'.

Present privacy governance regimes have repeatedly failed to safeguard this moral ecology of 'autonomy', and have threatened to erode not only individual liberty but also the very basis of democratic life.

Furthermore, according to the communitarian perspective, safeguarding privacy entails upholding the trust, transparency, and mutual respect that are essential for healthy online communities. When individual data disclosures have broader implications, such as when a user's shared contact list allows for the profiling of hundreds of other users, procedural consent-based regulations fail to consider these collective elements. (Brouwer, 2020).

From a different angle, critical theory, especially that created by Michel Foucault and, more recently, Shoshana Zuboff, analyzes the structural factors and power disparities that affect contemporary data environments. In his book "Discipline and Punish", (Foucault, 1995) concentrated on the idea of "governmentality" and the study of the panopticon. "Panopticon is a form of prison design which enables constant scrutiny of inmates without the inmates themselves knowing if they are being observed. The very presence of the panopticon exerts an influence on behavior. It is a low-cost means of surveillance and control" (Flavin (2023, p.2). The idea of "surveillance capitalism" has given this viewpoint an additional specs, which sees the commodification of human experience as the fundamental logic of the modern digital economy. The very collection of data by tech giants such as Amazon, Google, or Meta for the purpose of predicting and influencing consumer behavior for profit suggests how these companies view individuals as

a commodity for their data (Zuboff, 2019). By taking advantage of loopholes in privacy laws and co-opting notice and consent procedures, such organisations can exploit the imbalances in the system, turning individuals into passive data subjects rather than active rights holders.

Both the communitarian and critical viewpoints oppose the present governmental systems that place formal approval before actual agency. The two perspectives taken together highlight that data governance is inherently political and value-driven, rather than being neutral or merely technical. This study therefore applies Kantian Digital Autonomy and Rawlsian Justice as fairness to assess the GDPR and India's DPDP Act especially in context of AI.

3. Normative Foundations for Contemporary Data Governance

3.1 Kant's theory of Digital Autonomy

The Kantian ideas of autonomy and human dignity are among the most influential philosophical contributions to the way people perceive privacy. According to (Mponda, 2021) "For him, the wrongness or rightness of an action depends on whether it respects duty." "Kant's practical philosophy has resources with which we can get a good handle on the problems of ungrounded modern individuals, the importance of privacy for human beings, and the structure of (including the differences between) the ethical and judicial rights and duties regarding privacy."

According to Immanuel Kant's moral philosophy, notably his definition of the "Categorical Imperative" which says that, "a categorical imperative does not depend upon my desires or wants, these are necessary and always binding and are the ought's that determine what our moral duties are." (Johnson, 2024). The Kantian view has important implications for the present technology-driven world. When individuals' personal data/sensitive information is collected, stored, processed, and commercialized without meaningful consent or understanding, it reduces people to mere data-fetching centers for algorithmic processing for organizational or business interests. This instrumentalization of humans goes against the very notion of 'morality' as suggested by Kant. Moreover, the concept of 'autonomy' as provided by Kant is not a mere condition of non-interference, but a condition of rational self-legislation. It implies that individuals must have both the capacity and the opportunity to govern their informational boundaries in a manner consistent with their own rational values and life goals. (Ülgen, 2017) argues that "Kantian ethics make two distinct contributions to the debate; First, they provide a human-centric ethical framework whereby human existence and capacity are at the center of a norm-creating moral philosophy guiding our understanding of moral conduct; second, the ultimate aim of Kantian ethics is practical philosophy that is relevant and applicable to achieving moral conduct." However, Kant's idea of morality and autonomy are undermined by the current privacy practices, such as pre-ticked boxes, excessively complicated consent forms, and dark patterns, which manipulate user behavior rather than allowing for an informed/ genuine choice.

Therefore, in adapting a Kantian approach, it is necessary that privacy frameworks are developed in a manner that respects the moral agency of individuals and fosters a system where people can make informed and deliberate decisions about their data; hence, prioritizing AUTONOMY and fairness, not because law dictates so, but because it IS a moral imperative.

3.2 Rawl's Theory

The fairness and equity of digital governance systems are evaluated using John Rawls' political philosophy, particularly given in his groundbreaking book "A Theory of Justice". Based on Rawls (1999) notion of "justice as fairness", a fair institution is one that rational people would select when functioning behind a "veil of ignorance", meaning that they are unaware of their own social, economic, or personal situation. He asserts that fairness can only be attained if one arrives at an "original position". Within this study, Rawls provides the normative basis for assessing whether privacy governance distributes both the benefits and burdens of AI fairly across society, particularly for individuals and groups most vulnerable to algorithmic decision making.

According to (Douglas, 2015), "The original position is meant to represent the perspective of the noumenal self, the free and equal rational being whose choices are not influenced by prejudice or circumstance". Rawl's theory gives helpful insights into the creation of cybersecurity and privacy frameworks when applied to the digital realm, notably in light of the increasing inequalities and power imbalances created by algorithmic systems and other modern technologies. "Therefore, the Rawlsian difference principle mandates that the fundamental framework of society be governed in such a manner that the disparity in the possibility of acquiring the fundamental elements of well-being, income, and power is reserved for the advantage of the most disadvantaged". (Nurhayati, 2021, p. 32) The present-day widespread use of discriminatory profiling, algorithmic bias, and opaque automated decision-making demonstrates a striking failure to incorporate Rawlsian logic into current data governance structures.

The three principles Rawls outlined are still essential and applicable to maintaining the democratic legitimacy of modern digital institutions. (Westerstrand, 2025). The framework stresses that autonomous systems should be created in such a way that people would feel secure in accepting them from behind the "veil of ignorance", which means that these systems should protect fundamental liberties, fairness, equality of opportunity, and the difference principle by design, even when users are unaware or have unequal power. This framework emphasizes that the erosion of privacy caused by opaque decision-making, algorithmic control, or behavioral manipulation is essentially a violation of Rawlsian justice because these systems restrict the freedom of thought, association, and self-formation while failing to safeguard the most vulnerable (Ali, 2024).

The question of digital privacy is also addressed by Rawls's concept of "fair" equality of opportunity. People's access to credit, healthcare, education, and even employment may be subtly restricted by the use of algorithms and AI-based technology, which leads to algorithmic filtering, dynamic pricing, and predictive analytics that they are unaware of or unable to recourse. The Rawlsian perspective that people should have a 'real' chance to live their lives free of arbitrary restrictions is violated by these subtle kinds of exclusion, even if they are permitted by law or done for efficiency.

In Rawls' perspective, a fair approach to privacy would include transparency, fair audits, and algorithmic accountability mechanisms to maintain a level playing field in the digital world.

Rawls places an emphasis on reflective equilibrium and public reason in terms of institutional design, which suggests that government bodies should be democratically legitimate and subject to continuous ethical review. They shouldn't only be driven by market convenience or by technologically mandated privacy frameworks. All stakeholders, particularly individuals most affected by technological systems, should be involved in their development.

Taken together, Kantian Digital Autonomy and Rawlsian Justice as fairness provide the principal evaluative framework for this study. While Kant assess whether privacy laws preserve individual autonomy, dignity, and meaningful consent. Rawls on the other hand evaluates whether contemporary privacy governance promotes institutional fairness, equality of opportunity, and protection for the least advantaged. These perspectives provide the normative basis for the comparative analysis of the GDPR and India's DPDP

4. Jurisprudential Evaluation of Contemporary Privacy Frameworks

The philosophical discussion on privacy is centered on the concept of individual autonomy, which is the ability of individuals to manage their personal sphere, choose what to, to whom to disclose, and set the terms of such disclosure of their data. The concept of autonomy has always been the 'normative' core of privacy theory as seen in, Warren and Brandeis's definition of privacy of "right to be let alone", Alan Westin's description of "informational self-determination" and then Kant's theory of Autonomy and Rawl's theory of justice as fairness; and then Zuboff's panopticon theory grounded in utilization of modern technology for surveillance, explains more about the need of modern privacy governance regime than one could have anticipated. .

4.1 OECD Guidelines and UN principles on privacy

Building upon the jurisprudential evolution of privacy, International organisations such as OECD and UN gradually translated these philosophical principles into these normative standards for privacy in their Privacy guidelines. The OECD guidelines on the Protections of Privacy and Transborder Flows of Personal Data and the United National Principles on Personal Data Protection (2018) represent important International efforts to establish common principles for global privacy governance in response to data commodification, ubiquitous surveillance and Digital manipulation. Both of these regulatory tools have a similar approach to data privacy, consisting of principles such as Fair and Legitimate processing, purpose specified processing of data, Transparency in collection of data, Accountability, Fairness, setting timeline for retention of data, restriction on the amount of data collection, No-resharing of data with other parties, and lastly maintaining the confidentiality of the data so collected.

Central to the principles proposed by both OECD and UN, is the notice and consent mechanism: a model that is repeatedly invoked as the procedural embodiment of autonomy whose roots lied in the philosophical contentions of Westin. In theory, these principles do empower individuals to exert control over their personal data in the digital realm, and they also aligns with the Kantian moral imperative of treating individuals as ends in themselves and not as means to an end, and the imperative of the early philosophers to determine for themselves when, how, and to what extent their data should be utilized, shared, or collected about them.

However, viewing autonomy as just “informed consent” is insufficient. “It is also often treated as a truism that these requirements are to be justified by the principle of respect for autonomy. However, whilst this view is still widely accepted, it has recently been brought into question, with critics suggesting that informed consent requirements are neither necessary nor sufficient for safeguarding individual autonomy in critical spheres”. (Pugh, 2020, Ch.6). It posits a legal fiction that people are able to exercise agency in technologically complex and commercially opaque systems, that they have a full understanding of the ramifications of sharing their data, and that they are in a position to meaningfully advocate for their digital rights. Whereas the reality is far from it. The current technologies, along with autonomous systems, leave individuals uninformed of when and how their data is processed and collected. Interestingly, not just individuals, even the creators of these systems fail to know the working of algorithms, creating the ‘black-box problem’ and a lack of transparency. “The technical language is often mathematical, precise, and somewhat rigid, whereas the language describing social norms is flexible and less precise. There are substantive differences in scope, in what is considered personal information, in what is considered a privacy threat, in the protection required, and in the data formats the normative and technical conceptions contemplate. With such divergent foundations, it is difficult to reason about how these conceptions of privacy interact, or, more critically, whether they are in agreement at all.” (Nissim & Wood, 2018, p. 2). Viewing this in parallel to Kantian theory of Digital Autonomy, the ability to make a rational, thoughtful, and dignified choice is ignored conveniently in present digitalized environment, leaving users ‘alleged’ consent to be neither informed nor freely given. As procedural protections, notice and choice procedures are no longer sufficient. The essential structure of technological systems must be redesigned in order to restore the environment in which people are able to make moral decisions.

Accordingly, both the OECD guidelines and UN privacy principles reflect the continued dominance of informational self-determination within International privacy governance, a model that later influenced legislative frameworks such as Europe’s GDPR and India’s DPDP Act. The following section of the study therefore examines the GDPR and DPDP act using the rich normative conception of privacy, grounded in Kantian Digital Autonomy and Rawlsian justice and fairness especially in the present AI mediated society.

4.2 Data Privacy Regulations: Europe, and India

The General Data Protection Regulation (GDPR) Europe represents the first comprehensive data protection law in the world that had setup a standard for privacy regulations around the globe. It was enacted in 2016 by the European Union and came into

force in May 2018, before the widespread deployment of generative AI and advanced algorithmic systems.

“The objective of the GDPR was to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data, in particular the movement and the processing of their personal data.” (GDPR, 2016, Art. 1). The GDPR is built on the pledge of regaining individual autonomy, by informing individuals prior to the processing and collection “about the processing, such as its purposes, the types of data collected, the recipients, and their data protection rights.” (Articles 5–11) of the GDPR provide for the principles for the processing of Data, which are well aligned with the OECD guidelines. Article 9 of the act categorically provides for the processing of special categories of personal data. At the core of GDPR lies the promise of restoring individual autonomy, a right explicitly entrenched in its fundamental principles and operationalized via mechanisms such as data portability (Article 20), the right to access (Article 15), the right to erasure (Article 17), and informed consent (Article 6(1)(a)).

When viewed through the perspective of philosophical dedication to autonomy and self-determination, GDPR presents a complicated picture. GDPR is based on the assumption that people can make educated and rational decisions about how their data is used, thereby using the Westin’s “notice-and-consent” model. (Recitals 32, 42, and Art. 7). However, this framework is increasingly becoming inadequate in the present times of algorithmic transparency, behavioral nudging, and asymmetric information transfer. It also leads to undermining the Kantian Digital Autonomy principle. The GDPR assumes that the data subject is a rational and ethical actor who is able to engage with data infrastructures in a meaningful way which is what Kantian ethics argues. Regardless of the fact that regulation mandate the consent be voluntary, explicit, informed, and clear, empirical data indicates that the majority of consumers “agree” even when they lack a realistic choice or a complete knowledge of what they are agreeing to. (Utz et al., 2019)

Furthermore, the GDPR’s approach to controlling emerging algorithmic technologies like artificial intelligence and predictive profiling is not as effective as its capacity to regulate traditional data processing. The right of individuals not to be subject to judgments made only by automated systems is granted by Article 22, but the article’s efficacy is undermined by wide exceptions, particularly when the processing is permitted by legislation or is based on specific agreement. Additionally, it is still uncertain under the law what constitutes “meaningful information about the logic involved”, and it is seldom used in reality where individuals are often forced to make decisions that they don’t comprehend or disagree with, bringing up significant issues about transparency and procedural fairness going against the very practise of Rawls’s Justice as Fairness theory. While the regulation does introduce important safeguards against automated decision-making, its reliance on procedural right assumes that individuals possess relatively equal capacities to understand, challenge, and exercise those rights. In reality, Informational asymmetries, unequal digital literacy, and the concentration of technological power meant that vulnerable individuals often bear a disproportionate share of algorithmic harms. Consequently, the GDPR only partially satisfies Rawlsian Justice as Fairness by protecting Formal Rights without fully addressing structural inequalities within digital ecosystem.

The central question therefore, is whether India's DPDP Act, enacted almost seven years after the adoption of GDPR and after the transformative rise of AI, reflects a more evolved normative conception of privacy than the GDPR?

The Digital Personal Data Protection Act, 2023 (DPDP Act) of India is a long-awaited step towards establishing a comprehensive data protection framework. The law, which is based on the notion of “consent as a rule”, places a strong emphasis on data minimization, purpose limitation, notice, and the rights of individuals over their own data following the architecture of GDPR very closely, which shows that even after 7 years, with such accelerated rate of adoption of AI, privacy is still protected via the self-determination.

Beginning with the section 6 of the act, the legal foundation for handling personal data must be consent, which must be “free, specific, informed, unconditional, and unambiguous with a clear affirmative action”(DPDP, 2023, sec. 6). Westin's fundamental notion of privacy as individual control is reflected in this, which also reflects Kantian ethics by assuming that the data principal is a rational moral agent who can provide real consent. In reality, though, this notion rapidly falls apart.

The Act also establishes a condition of “legitimate use” under Section 7 of the act for purposes such as medical emergencies, state functions, and employment-related applications, but the definition of the term is vague and susceptible to abuse. (DPDP, 2023, Sec. 7). By enabling data to be processed without a clear, informed decision, this compromises the independence and Autonomy that it intends to protect. From a Rawlsian perspective, the act also raises equally significant concerns regarding fairness and institutional justice, such as exemptions that are given in the legislation relating to state functions, employment, and legitimate uses. These exemptions disproportionately affect individuals who possess limited bargaining power or digital literacy. Rather than making an effort to reduce structural inequalities, the act assumes that formal legal rights are sufficient to ensure fairness. Consequently, the burdens associated with opaque data processing and algorithmic decision-making are most likely to be borne by the least advantaged members, i.e. someone who doesn't possess as much bargaining power or someone with limited digital literacy or a member of minority, which goes against the Rawl's different principle and his conception of justice as fairness.

Additionally, it is noteworthy that the act lacks on account of modern technology and algorithmic transparency requirements and restrictions. The legislation in itself is silent on the issues presented through modern technology when employed for algorithmic profiling and focused behavioral manipulation. However, the extended DPDP rules, enacted in 2025 entailed an additional responsibility over significant data fiduciary to act with added due diligence in utilization of automated algorithms (DPDP Rules, 2025, Sec. 13); the applicability and adherence to these rules are extended to 2027. Furthermore, the Act also does not require data fiduciaries to provide a clear explanation of how profiling or predictive analytics are used, effectively obscuring the digital processes that have the greatest impact on individual dignity. The act also excludes any data in public sphere. (DPDP, 2023, Sec.3)

This presents moral concerns from a Kantian viewpoint. Systems that rely on unclear data extraction, manipulation, or nudging, frequently without the knowledge of data principals, violate the duty to treat people as ends in themselves rather than merely as means to corporate or governmental objectives. The DPDP Act does allow such treatment under a variety of vague justification, such as “public interest” and “reasonable

expectations”, but it does not mandate comparable transparency or procedural safeguards.

The rights provided under the Act is likewise underdeveloped. Although it introduces rights to correction, erasure, and grievance redressal (DPDP, 2023, Sec.12-14), it excludes the right to data portability and, more importantly, the right to object to automated decision-making. This implies that, in reality, either India lacks the resources to effectively regulate algorithmic profiling, behavioral targeting, or digital discrimination or it is used by the system itself in ‘public interest’ thereby affirming with the Zuboff’s theory of surveillance.

From a legislative point of view, the DPDP Act appears to be an effort to balance state authority, economic innovation, and the protection of personal data, but the balance is surely off. The act does not prioritize the normative commitments to autonomy nor the law prioritizes practical flexibility, which leaves people structurally vulnerable to both corporate surveillance and governmental overreach.

5. Reconstructing Privacy Governance through Jurisprudential Foundations

The comparative evaluation of the GDPR and DPDP, demonstrates that although both the GDPR and India’s DPDP Act, as evaluated in the paper, is at best technically compliant (to the present privacy standards), and at its worst, ethically devoid (from the philosophical point of view), owing to the obvious disconnect between the philosophical underpinnings of privacy and current privacy governance systems especially in trying to regulate the AI driven ecosystem using the same regulation. Despite recognizing the right to privacy under International covenants and by various jurisdictions such as India and EU, the actual exercise of this right often lacks a strong normative foundation. As previously mentioned in the paper, privacy frameworks have increasingly relied on administrative methods such as impact assessments, consent forms, and procedural checklists. These tools, though performing vital operational tasks, hardly represent the profound philosophical beliefs that have historically backed the notion of privacy as a moral, democratic, and existential right. The current privacy governance regime necessitates a paradigm change that goes beyond the conventional distinction between ethical principles and technological design. Autonomy, dignity, and the right to self-determination are philosophical values that must now be put into practice via real technological and legal frameworks that govern how data is collected, processed, shared, and safeguarded, rather than being just theoretical ethical ideals. (Graef et al., 2023).

The traditional notice-and-consent model is now mostly obsolete due to the development of surveillance capitalism, machine learning, and algorithmic systems. (Magrani, 2019). In order to accommodate new philosophical writings that discuss the changing nature of technological harms, current regulatory systems must be adaptable.

A reconstructed model of Privacy governance must therefore move beyond procedural compliance and incorporate the normative commitments. From the Rawlsian perspective, his notion of ‘justice as fairness’ introduces the thought experiment of the “original position”, in which rules are established behind a “veil of ignorance”, to ensure fairness to everyone, particularly the least fortunate. When translated to data governance, this means that legislation should be drafted to protect those who are most at risk from data-

driven dangers, such as algorithmic discrimination, data exclusion, or surveillance bias. (Iwan & Sojka, 2024). However, existing regulatory frameworks fail to adopt to this obligation. Legislative efforts around the globe are often focused on the average, competent user, ignoring the disproportionate impact that predictive analytics or algorithmic decision making can have, on racial minorities, low-income groups, and people who are outside of the major data categories. (Alderman et al., 2024). Therefore, in adoption of the Rawlsian theory, governments and their delegated authorities are to carry out impact evaluations not just for compliance purposes, but also for justice, making sure that data governance frameworks proactively protect marginalized identities from structural algorithmic injustices.

From a Kantian perspective, governance frameworks must preserve meaningful digital autonomy by ensuring that individuals remain genuine moral agents rather than passive sources of behavioural data. Consent therefore should represent an informed and deliberative exercise of self-governance rather than a formal legal prerequisite satisfied through opaque interfaces or manipulative design practises. “Mandated equity audits, data justice review boards, or bias-resilient standards in AI procurement and public sector technologies may be ways to incorporate this into legislation”. (Agbabiaka et al., 2025)

Furthermore, Regulatory frameworks still underestimate the philosophical pluralism that has been developed by philosophers such as Judith Jarvis Thomson. Contrary to any monolithic idea of privacy, Thomson contended that privacy comprises a web of rights. In order to integrate the pluralistic view of Thomson, Law must establish flexible, domain-specific protections that account for this intricacy. For example, healthcare consent standards may have higher requirements than those used in e-commerce because the inherent nature of the data shared is taken into account in addition to risk assessments. Therefore, rebuilding governance must adopt context-sensitive safeguards that recognizes varying level of informational sensitivity and shall exercise changing incentives to encourage appropriate data collection such as limiting data retention windows, taxing data brokerage profits, or mandating fiduciary duties for platforms that maintain personal data. (Perucci & Swanson, 2024). It might also entail treating personal data not as a commodity to be commercialized, but as an extension of one’s identity that merits unalienable protection.

According to (Nissim & Wood, 2018), “Adopting an understanding of privacy that is consistent across its technical and normative dimensions will be critical to ensuring personal data is adequately safeguarded over the long term.” “They are neither purely legal nor purely technical, but rather a multi-dimensional combination of the two. Understanding the hybrid nature of these concepts and developing tools for implementing them is necessary to bridge the gaps between the current legal and technical understanding of privacy.” Therefore, the paper recommends, a hybrid model which will make it possible to reconcile what should be protected (normatively) with what can be protected (technically). Additionally, such a model may pave the way for more scientific accountability in privacy law and more ethical awareness in technical systems.

Additionally, hybrid models offer a tiered approach to access that is modeled after the Privacy Tools Project and classifies various kinds of data access, from open differential privacy tools to secure data enclaves, according to their level of sensitivity and potential risks. (The Royal Society & Noble, 2023). This is especially important in algorithmic systems, where the initial scope of consent may be far surpassed by data sharing and AI

model rendering retroactive regulation ineffective. At the center of this discussion is the urgent need to revive ‘contextual integrity’ as a formalizable, hybrid concept. According to Nissenbaum’s concept of Contextual integrity, privacy is protected if data transfers comply with contextual norms. According to recent studies, these standards maybe translated into machine-readable forms, allowing automated systems to identify data transfers that go against contextual expectations. (Hoel et al., 2020). This could serve as a connection between the technical execution of policy compliance and normative concepts of legitimate expectation. The future of privacy laws depends on the integration of legislative reform and technological innovation, not on choosing between them.

6. Conclusion

In today’s digital age where our lives are dependent on technology and we are surrounded by a pervasive surveillance infrastructure, algorithms are making our decisions based on our behavior and activities; the fundamental moral of privacy has transformed. Privacy went from a simple matter of secrecy or information control to a moral battle for human dignity, freedom, and justice. The present governance frameworks around privacy have failed to close the ethical gaps created due to massive adoption and integration of automative technology, and include the normative understandings of privacy as understood by classical and modern philosophical schools. The core principle of privacy, as seen in many jurisprudential lenses analyzed throughout this paper, remains the same: whether it is Rawls’ concept of justice, the Kant’s emphasis on rational agency or Nissenbaum’s contextual integrity. All the jurisprudential lenses seem to point to one thing collectively i.e., in a democratic society, privacy is essential for the individual to flourish.

However, in the contemporary privacy frameworks, privacy is seen as a procedural safeguard rather than a fundamental one. The frameworks continue to adopt Westin’s notice and consent mechanism; it is insufficient in the face of behavioral manipulation, dark patterns, and opaque algorithmic designs. As assessed in the paper, laws like the DPDP Act and the GDPR use reactive approaches that do not integrate or adhere to other philosophical underpinnings of privacy, which are evaluated using Kant’s Digital Autonomy theory and Rawls’s Justice as Fairness. After assessment, the paper proposes a hybrid governance model that integrates the ethical tenets of legal philosophy with the practical capabilities of privacy-enhancing technologies. To genuinely prioritize privacy and autonomy in such a framework, privacy must be integrated at both the architectural and institutional levels, not merely be addressed as a regulatory afterthought or a technical “privacy by design” idea. This would facilitate proactive governance, which would safeguard autonomy. Real measures to achieve this objective include requiring algorithmic bias and equity audits before deployment, establishing data fiduciary responsibilities that legally compel companies to safeguard users’ interests, implementing context-aware privacy tools modeled after Nissenbaum’s contextual integrity, and maintaining institutional independence in privacy regulation to prevent regulatory constraint. These ethical commitments can only be translated into enforceable standards through interdisciplinary collaboration between law, philosophy, and computer science, thereby guaranteeing that privacy is maintained in both theory and reality.

Future study should concentrate on operationalizing this hybrid model by investigating how ethical considerations can be effectively included in technological design and how legislation may be modified to promote such integration. To ensure that privacy remains strong in the face of constantly changing digital threats, a more comprehensive, interdisciplinary examination combining law, philosophy, and computer science is required.

Disclosure of Interest. The Authors have no competing interest to declare that are relevant to this paper.

References

- Birch, K., Cochrane, D., Ward, C.: *Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech*. *Big Data & Society*, 8(1) (2021)
- Nishnianidze, A. : *Surveillance in the digital age*. *European Scientific Journal* 20(37), 1-25 (2024)
- Moore, B.: *Privacy and the communitarian self* (Unpublished master's thesis). Victoria University of Wellington. (2021) https://openaccess.wgtn.ac.nz/articles/thesis/Privacy_and_the_Communitarian_Self/17132267 last accessed 17/02/26
- Adadi, A. : *A survey on data-efficient algorithms in big data era*. *Journal of Big Data*, 8(1), Article 24 (2021).
- Agbabiaka, O., Ojo, A., Connolly, N.: *Requirements for trustworthy AI-enabled automated decision-making in the public sector: A systematic review*. *Technological Forecasting and Social Change*, 215, 124076 (2025).
- Alderman, J. E., Palmer, J., Laws, E., McCradden, M. D., Ordish, J., Ghassemi, M., Pfohl, S. R., Rostamzadeh, N., Cole-Lewis, H., Glocker, B., Calvert, M., Pollard, T. J., Gill, J., Gath, J., Adebajo, A., Beng, J., Leung, C. H., Kuku, S., Farmer, L., Liu, X.: *Tackling algorithmic bias and promoting transparency in health datasets: the STANDING Together consensus recommendations*. *The Lancet Digital Health*, 7(1) e64–e88 (2024).
- Ali, M.Y. : *Ethics of technological futures: John Rawls' framework*. *Journal of Futures Studies*, 28(3), 1–11. (2024). <https://jfsdigital.org/articles-and-essays/2024-2/vol-28-no-3-march-2024/ethics-of-technological-futures-john-rawls-framework/>
- Becker, M.: *Privacy in the digital age: Comparing and contrasting individual versus social approaches towards privacy*. *Ethics and Information Technology*, 21(4), 307–317 (2019)
- Board of Governors of the Federal Reserve System. (2006). *FTC Act Section 5: Unfair or deceptive acts and practices* ([Consumer Compliance Handbook] Appendix I-V). Retrieved July 18, 2025 from <https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf> last accessed 10/02/26
- Bycer, M. L. : *Understanding the 1890 Warren and Brandeis "The Right to Privacy" article*. National Paralegal College. (n.d.). <https://juris.nationalparalegal.edu/UnderstandingWarrenBrandeis.aspx> last accessed 14/02/26

Centers for Disease Control and Prevention: *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*. U.S. Department of Health and Human Services. (2024, October). <https://www.cdc.gov/php/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html> last accessed 14/02/26

Clements, P., Formosa, P. : *Beyond ideal theory: Foundations for a critical Rawlsian theory of climate justice*. *New Political Science*, 43(4), 486–505 (2021).

Currie, M., Knox, J., McGregor, C.: *Introduction: Data justice and the right to the city*. In *Data justice and the right to the city* (pp. 1–22). Edinburgh University Press, (2022).

Lindsay, D.: *An Exploration Of The Conceptual Basis Of Privacy And The Implications For The Future Of Australian Privacy Law*. *Melbourne University Law Review*, 29, 161–167 (2005)

De Brouwer, S.: *Privacy self-management and the issue of privacy externalities: of thwarted expectations, and harmful exploitation*. *Internet Policy Review*, 9(4) (2020).

Ding, X., Huang, H. : *For whom is privacy policy written? A new understanding of privacy policies*. *Computer Law & Security Review*, 55, Article 106072 (2024).

Douglas, D. M. : *Towards a just and fair Internet: Applying Rawls' principles of justice to Internet regulation*. *Ethics and Information Technology*, 17(1), 57–64 (2015).

European Commission: *What are the main aspects of the General Data Protection Regulation (GDPR) that a public administration should be aware of?* European Union. Retrieved: https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_en last accessed 20/02/26

European Parliamentary Research Service: *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence* (PE 656.305) 9(2020). European Parliament.

([https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU\(2020\)656305_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf)) last accessed 08/02/26

European Union: *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. *Official Journal of the European Union*, L 119, 1–88. (2016). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>

Federal Trade Commission: *Children's Online Privacy Protection Rule (16 C.F.R. § 312)*. Federal Register, 64 Fed. Reg. 59900–59954; as amended (1999). <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> last accessed 20/02/25

Federal Trade Commission: *FTC provides guidance on updated Safeguards Rule*. FTC News. <https://www.ftc.gov/news-events/news/press-releases/2025/06/ftc-provides-guidance-updated-safeguards-rule> last accessed 20/02/25

Flavin, M.: *"I kind of feel resigned to the fact": A Foucauldian perspective on data privacy and social media*. *Irish Journal of Technology Enhanced Learning*, 7(1), 48–63 (2023).

Foucault, M.: *Discipline and punish: The birth of the prison* (2nd Vintage Books ed.; A. Sheridan, Trans.). Vintage Books. (1995)

- Garrett, J. E. : *How Rawls could support a right to privacy*. Western Kentucky University (2005).
- Government of India: *The Digital Personal Data Protection Act, 2023 (No. 22 of 2023)*. Ministry of Law and Justice. <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf> last accessed 23/02/26
- Graef, I., Petročnik, T., Tombal, T. : *Conceptualizing autonomy in an era of collective data processing: From theory to practice*. Deleted Journal, 2(2) (2023)
- Hoel, T., Chen, W., Pawlowski, J. M. : *Making context the central concept in privacy engineering*. Research and Practice in Technology Enhanced Learning, 15(1) (2020).
- Hoofnagle, C. J., Urban, J. M.: *Alan Westin's privacy homo economicus*. Wake Forest Law Review, 49(2), 261-317 (UC Berkeley Public Law Research Paper No. 2434800) (2014)
- Iwan-Sojka, D. : *The inclusive data governance models for algorithms – a dream of the already convinced or a realistic way of action?* Information & Communications Technology Law, 1–14 (2024).
- Jiang, Y., Yu, X., Qin, Y. : *Unraveling the balance between personal data protection and public interest: a theoretical framework and its empirical application in personal data processing*. Journal of Chinese Governance, 1–22. (2025).
- Johnson, R. N. : *Kant's moral philosophy*. In E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy (Winter 2004 ed.). Metaphysics Research Lab, Stanford University. (2004). <https://plato.stanford.edu/entries/kant-moral/> last accessed 21/03/26
- Kathuria, Y., Ruhani, V., Vandana, M. T., Jain, V.: *Protecting data privacy in the age of AI: A comparative analysis of legal approaches across different jurisdictions*. In *ETLTC 2024 International Conference Series on ICT, Entertainment Technologies, and Intelligent Information Management in Education and Industry*, volume 3220, Article 040007. AIP Conference Proceedings. (2024)
- Kisselburgh, L., Beever, J.: *The Ethics of Privacy in Research and Design: Principles, practices, and potential*. In Springer eBooks (pp. 395–426) (2022).
- Kramer, I. R.: *The birth of privacy law: A century since Warren and Brandeis*. Catholic University Law Review, 39(3), 703–724 (1990). <https://scholarship.law.edu/lawreview/vol39/iss3/3> last accessed 21/03/26
- Magrani, E.: *New perspectives on ethics and the laws of artificial intelligence*. Internet Policy Review, 8(3) (2019).
- Marky, K. : *Data collection is not mostly harmless: An introduction to privacy theories and basics*. In N. Gerber, A. Stöver, & K. Marky (Eds.), *Human factors in privacy research* (pp. 3–10) (2023). Springer.
- Mason, S.: *Exploring privacy from a philosophical perspective: Conceptual and normative dimensions*. In S. Gutwirth, R. Leenes (Eds.), *Privacy and data protection: Philosophical, legal, and technological perspectives* (pp. 23–45) (2024). Springer.
- Rohlf, M.: *Kant's moral philosophy*. In E. N. Zalta & U. Nodelman (Eds.), The Stanford Encyclopedia of Philosophy (Fall 2024 ed.). Metaphysics Research Lab, Stanford University (2022). <https://plato.stanford.edu/entries/kant-moral/> last accessed 25/03/26
- Mponda, B.: *Information and privacy in the social media: A Kantian perspective*. (Unpublished Bachelor's dissertation), University of Malawi (2021) <https://www.researchgate.net/publication/354444444>

- searchgate.net/publication/351588407_INFORMATION_AND_PRIVACY_IN_THE_SOCIAL_MEDIA_A_KANTIAN_PERSPECTIVE last accessed 24/03/26
- Nishnianidze, A.: Surveillance in the digital age. *European Scientific Journal*, 20(37), 1–25 (2024)
- Nissenbaum, H.: *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press (2009).
- Nissim, K., Wood, A.: *Is privacy privacy? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2128), Article 20170358 (2018).
- Organisation for Economic Co-operation and Development (OECD): *Guidelines on the protection of privacy and transborder flows of personal data* (Recommendation of the OECD Council C(80)58(Final)). OECD (1980). https://www.oecd.org/content/dam/oecd/en/publications/reports/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f/9789264196391-en.pdf last accessed 30/03/26
- Orwell, G.: 1984. Secker & Warburg, London (1949)
- Owen, A., Matthews, A.: *Privacy rights and interoperability: A comparative study of regulations* [Preprint]. ResearchGate.(2024) https://www.researchgate.net/publication/389687742_Privacy_Rights_and_Interoperability_A_Comparative_Study_of_Regulations last accessed 02/04/26
- Parrilli, D.M.: *Defining a Privacy Ethical Framework for Service Design*. Springer series in design and innovation 89–121 (2024).
- Perucci, F., Swanson, E.: *Building trust and facilitating use of data*. Statistical Journal of the IAOS, 40(1), 71–79. (2024)
- Pugh, J.: *Informed consent, autonomy, and beliefs*. In: *Autonomy, rationality, and contemporary bioethics*, Chap. 6. 117–138, Oxford University Press, oxford (2020). <https://www.ncbi.nlm.nih.gov/books/NBK556864/> last accessed 02/04/26
- Rawls, J.: *A theory of justice* Rev. edn. Harvard University Press, Cambridge, MA (1999).
- Richards, N., Hartzog, W.: *Taking Trust Seriously in Privacy Law*. Stanford Technology Law Review 19, 431–471 (2016). <https://law.stanford.edu/wp-content/uploads/2017/11/Taking-Trust-Seriously-in-Privacy-Law.pdf> last accessed 04/04/26
- Sabr, A., Jubair, A.: *Perspective of Dystopian Society based on George Orwell's 1984*. Research Journal of English. 9, 288–304 (2024).
- Said, M. Y., Nurhayati, Y. (2021). *A review on Rawls' theory of justice*. ResearchGate. https://www.researchgate.net/publication/351178494_A_REVIEW_ON_RAWLS_THEORY_OF_JUSTICE last accessed 06/04/26
- Sandel, M. J.: *Liberalism and the limits of justice*, 2nd edn. Cambridge University Press, Cambridge (2012)
- Sandel, M. J.: *Political Liberalism [Review of Political Liberalism, by J. Rawls]*. Harvard Law Review, 107(7), 1765–1794 (1994) https://scholar.harvard.edu/files/sandel/files/political_liberalism.pdf last accessed 07/04/26

Tavani, H. T.: *Philosophical Theories of Privacy: Implications for An Adequate Online Privacy Policy*. *Metaphilosophy* 38 (1) 1–22 (2007).

The Decision Lab: Michael Sandel, *The celebrity Political Philosophers* <https://thedeisionlab.com/thinkers/philosophy/michael-sandel> last accessed 09/04/26

Seipp, D.: *The Right to privacy in nineteenth century America*. *Harvard Law Review*, 94(8), 1892–1910. (1981)

The Royal Society: *From privacy to partnership: The role of privacy enhancing technologies in data governance and collaborative analysis*. The Royal Society (2023). <https://royalsociety.org/privacy-enhancing-technologies> last accessed 10/04/26

Thomson, J.J.: *The right to privacy*. *Philosophy & Public Affairs*, 4(4), 295–314. (1975).

Torbert, P. M.: “Because it is wrong”: *An essay on the immorality and illegality of the online service contracts of Google and Facebook*. *Journal of Law, Technology & the Internet*, 12(1) (2021). <https://scholarlycommons.law.case.edu/jolti/vol12/iss1/2> last accessed 10/04/26

U.S. Department of Health & Human Services, Office for Civil Rights : *Covered entities and business associates: Fast facts* (2024). <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html> last accessed 10/04/26

Ülgen, Ö.: *Kantian ethics in the age of artificial intelligence and robotics*. *QIL, Zoom-in*, 43, 59–83. *Questions of International Law* (2017). <https://www.open-access.bcu.ac.uk/5579/> last accessed 10/04/26

United Nations: *UN Principles on Personal Data Protection & Privacy*. United Nations. (2018) https://unsceeb.org/sites/default/files/imported_files/UN-Principles-on-Personal-Data-Protection-Privacy-2018_0.pdf last accessed 11/04/26

General Assembly, United Nations: *Universal Declaration of Human Rights*. United Nations. (1948) https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf Last accessed 11/04/26

General Assembly, United Nations: *International Covenant on Civil and Political Rights*. United Nations Treaty Series, 999, 171. (1966) <https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf> Last accessed 11/04/26

University of Oxford, Institute for Ethics in AI: *Ethics in AI colloquium with Frank Pasquale: Machines judging humans* (2021). <https://www.philosophy.ox.ac.uk/event/ethics-in-ai-colloquium-with-frank-pasquale-machines-judging-humans> Last accessed 11/04/26

Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: *(Un)informed consent: Studying GDPR consent notices in the field*. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)* (pp. 973–990). ACM, New York (2019).

Varden, H.: *Kant and privacy*. In: Lyssy A, Yeomans, C. (eds.), *Kant on morality, humanity, and legality: Practical dimensions of normativity*, 229–252. Palgrave Macmillan, cham (2020).

Wenar, L.: *John Rawls*. In: Zalta, E.N., Nodelman, U. (eds.), *The Stanford Encyclopedia of Philosophy*, Summer 2021 edn. Metaphysics Research Lab, Stanford University, Stanford (2021). <https://plato.stanford.edu/archives/sum2021/entries/rawls/> last accessed 10/04/26

Westerstrand, S.: *Towards just democracies in the age of pervasive digital systems- a Rawlsian approach*. AI & Society (2025).

Westin, A. F.: Privacy and freedom. *Washington & Lee Law Review*, 25(1), 166–220 (1968). <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20> last accessed 11/04/26

Zuboff, S.: *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs, New York (2019)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

