



International Journal of Electronic Governance

ISSN online: 1742-7517 - ISSN print: 1742-7509

<https://www.inderscience.com/ijeg>

Indian approach to data rights: survey of social structures, and personal data protection regimes in India

P.R. Biju, O. Gayathri

DOI: [10.1504/IJEG.2025.10070152](https://doi.org/10.1504/IJEG.2025.10070152)

Article History:

Received:	08 September 2024
Last revised:	18 September 2024
Accepted:	20 January 2025
Published online:	18 April 2025

Indian approach to data rights: survey of social structures, and personal data protection regimes in India

P.R. Biju*

Department of Political Science,
Government Brennen College,
Thalassery, Kannur, 670106, Kerala, India
Email: bijugayu@gmail.com

*Corresponding author

O. Gayathri

Department of Political Science,
Government College Madappally,
Vadakara, Kozhikode, Kerala, 673102, India
Email: gayubijuspeak@gmail.com

Abstract: The research paper conducts comparative analysis of data protection frameworks and AI policies in India and various countries, and seeks to investigate their capability in safeguarding data rights and enforcing fiduciary responsibilities favourable to users with a focus on India. Deploying a mixed method approach, it explores classical theories of rights, property ownership, and data protection frameworks. It seeks to explain how data rights intersect with India's intricate social structure. The findings reveal shortcomings in India's common law jurisdiction, lacking tools to effectively address data rights and fiduciary responsibilities. The study suggests that policy drafts in India need to uphold the culture sensitivity of data governance, considering the nation's complex social dynamics and data trust principles needs to align with India's unique trust and relationship dynamics.

Keywords: artificial intelligence; data policy; fiduciary trust; structural oppression; data rights; algorithms; India; data trust.

Reference to this paper should be made as follows: Biju, P.R. and Gayathri, O. (2025) 'Indian approach to data rights: survey of social structures, and personal data protection regimes in India', *Int. J. Electronic Governance*, Vol. 17, No. 1, pp.51–85.

Biographical notes: P.R. Biju is an academic and author, currently serving as Professor of Political Science at Government Brennen College, Thalassery, Kerala, India. His wide-ranging research interests include the social implications of artificial intelligence, the societal effects of fake news, the cultural expressions of romance in India, the impact of internet pornography, and the role of social media in shaping political and social processes. His body of work, including *Political Internet* (Routledge, 2016), *Intimate Speakers* (Fingerprint!, 2017), *Selfie Sex* (Kalamos, 2018), *Slave Technology* (Rupa, 2019), *We Are Products* (Rupa, 2023), and *Automated Lies* (Palgrave, 2025),

reflects his diverse research expertise. He has also published numerous scholarly papers in leading journals such as *AI & Society* and the *Journal of Social Computing*. His current research deals with themes of love and democracy, as well as the influence of Hindu scriptures on contemporary views of artificial systems.

O. Gayathri is an accomplished academic in Political Science, currently serving as Professor at Government College Madappally, Kerala, India. With a PhD focused on women's movements, identity, and empowerment in Kerala, her research delves deeply into the intersection of women's studies, family politics, and public space. She has an extensive portfolio of publications, including papers in high-impact journals on artificial intelligence, algorithms, social media, and their implications for governance and women's movements. Additionally, she is a sought-after speaker, having presented papers at numerous national seminars, contributing significantly to the discourse on gender, social movements, and digital activism in India. Her work, both as a scholar and educator, continues to shape critical conversations around the role of women in political and public spheres.

1 Introduction

In the evolving landscape of data governance (Vial, 2023) and data privacy in AI technology (Torra, 2023), the conventional paradigm of data ownership (Raina and Palaniswami, 2021) has come under scrutiny due to its limitations in providing individuals with meaningful control over their personal data (Alfnes and Wasenden, 2022). Integrating fiduciary principles (Whitt, 2020) as an alternative framework to traditional data ownership models, hence gain currency. Fiduciary duties, grounded in the concept of trust and accountability, offer a unique perspective that aligns with the contemporary demand for enhanced data rights (Bailey and Goyal, 2019).

No country had explicitly applied fiduciary principles to data ownership and data rights on a widespread basis (Giannopoulou et al., 2022). However, there were discussions and proposals in various countries about treating personal data as a form of property and establishing fiduciary duties or rights for organisations that collect and process such data (AIBR, 2022; GDPR, 2018; DPDPB, 2023). Some scholars, policymakers, and advocacy groups have been exploring this approach as a potential way to empower individuals with more control over their personal data and to establish responsibilities for organisations handling that data (Bailey and Goyal, 2019; Whitt, 2020).

Central to this is the understanding that rights including ownership and property require sophistication in treating data as right. Numerous intellectual perspectives have been presented concerning how to view rights within human society. For instance, Hobbes (1651) posited that rights were established and acknowledged by the ruling authority, while Rousseau (1762) argued that a legitimate social contract should be based on the general will of the people, enabling them to create laws and rights that align with the common good. Locke (1689) maintained that governments were formed through a social contract to safeguard rights, and Paine (1791/2012) contended that rights were not

bestowed by the government but were inherent to every individual by virtue of their humanity.

Treating data ownership using a classical lens of rights is not sufficient to validate the claim to own data as right. Hence alternative proposals are advanced (Stepanov, 2020). Several countries are now viewing data as right and provides ownership rights through legal frameworks. Against this backdrop, it becomes imperative to comprehend the efforts made in national data and AI policy documents in India to safeguard the data rights of citizens in an increasingly datafied world that is yet to be fully realised in India. Within India's civil and legal laws, the concept of data as a right finds no recognition (Prasad, 2019)]. The country has produced several drafts of data policies, including

- 1 JBNSCR (2018)
- 2 DPDPB (2018)
- 3 NSAI (2018)
- 4 RAITF (2018)
- 5 PDPB (2019)
- 6 PRAI (2021)
- 7 JPCR (2021)
- 8 IDAUP (2022)
- 9 IDABNUP (2022)
- 10 DPDPB (2022)
- 11 DPDPA (2023).

This research undertakes an examination of these data policy drafts in India and investigates fiduciary principles to safeguard data ownership rights.

2 Review of literature

The implications of data (Kitchin, 2014) on human society's rights remain relatively unexplored (Schäfer and van Es, 2017). The growth of data collection has surged exponentially, progressively encroaching into private domains (Haupt, 2016). The act of yielding personal data (Quach et al., 2022), granting consent for its collection and use, often without a full understanding of its utilisation, all in exchange for ostensibly 'free' access to cherished products and services, has become a taken-for-granted norm (Burri, 2017). However, this practice has spawned discomfort, intensified by significant incidents involving mishandling and improper data utilisation (Durnell et al., 2020).

The challenge of governing data arises from the tension between its potential for beneficial applications, such as health research, and the potential to harm, such as algorithmic bias. Data is hailed for its transformative potential across sectors and industries, spanning from supply chain management (Chi et al., 2020) to medicine (Ali et al., 2018) to automobiles (Lugano, 2017), with the power to reshape business models (Duan et al., 2019), reshape labour landscapes (Schwartz et al., 2019), enhance performance (Wilson and Daugherty, 2018), and augment human capabilities (Dwivedi

et al., 2021). AI technologies like autonomous vehicles, smart assistants, and healthcare diagnostics are poised to revolutionise daily life (Manyika et al., 2017; Bostrom, 2014).

Various studies have, on the other, delved into the risks associated with the use of data based algorithmic decision-making (Craglia et al., 2021; Gekker and Hind, 2019; Lightfoot and Wisniewski, 2014). Recent literary works such as ‘The Costs of Connection’ (Couldry and Mejias, 2019), “Stand out of Our Light” (Williams, 2018), and “The Age of Surveillance Capitalism” (Zuboff, 2019) have illuminated the darker facets of technological advancements. A crucial aspect of these emerging concerns revolves around data’s impact on rights, especially its role in perpetuating discrimination (Boyd and Crawford, 2012; Eubanks, 2014; Gangadharan, 2014).

Data governance (Abraham et al., 2019) thus navigate the interests of individuals and society while handling vast sets of sensitive personal data and their custodians. Concepts like data ownership (Al-Khouri, 2012), data rights (Harris and Wyndham, 2015), and personal data as property (Hazel, 2020) hold significance here, sparking a substantial debate on data ownership in the data-driven society (Arrieta-Ibarra et al., 2018).

The conceptual difficulties surrounding ‘data ownership’ and ‘data rights’ have posed significant hurdles in data-related discussions (Hicks, 2023). The notion of ‘data ownership’ resonates intuitively (Risse, 2021), encapsulating the idea of data belonging to an individual. The motivations of this discourse include safeguarding privacy and ensuring individuals and organisations control their own data (Alafaa, 2021). The common sentiment is that individuals should wield authority over their data and should profit from its financial or political usage (Prince, 2017). High-profile incidents where data was employed for political purposes without consent have spurred strong reactions, reinforcing the call for data control and benefits (Cadwalladr and Harrison, 2018). However, ‘data ownership’ faces significant challenges, rendering it inadequate for establishing a comprehensive data management system to address mounting unease (McBride, 2018). These challenges necessitate thorough consideration and resolution to craft a more appropriate vision for such a system (Lund, 2011).

The concept of data ownership presents considerable challenges (Baron, 2012) due to data’s unique attributes that distinguish it from traditional tangible possessions subject to ownership (Lund, 2011). Data boasts a non-rivalrous nature (Jones and Tonetti, 2020), enabling sharing without depletion, unlike physical items where transfer implies loss of possession. For instance, compromised personal data retains access for the owner while falling into unauthorised hands. In contrast, selling a physical property like a house entails complete ownership transfer, barring further sales. Furthermore, data can pertain to multiple individuals, blurring the connection between data concerning a single individual and the notion of ownership (Fia, 2021). Genetic data about an individual, for example, also pertains to their family (Westendorf et al., 2018), while business-generated data inherently involves multiple individuals (Sivarajah et al., 2016). Personal data linked to an individual retains its connection even when transferred, further muddling ownership (Hummel et al., 2021).

The ambiguity about who should be deemed the data ‘owner’ raises questions about parallels with conventional property forms. In certain cases, the data ‘owner’ could be an entity holding an aggregated dataset encompassing numerous individuals (Hummel et al., 2021). These complexities underscore the lack of a solid legal foundation for the concept of data ownership in both common and civil law systems (Yu and Zhao, 2019). Legal definitions of ‘data’ are lacking (Gellert, 2020), with only personal data receiving clear clarification. The definition of ‘personal data’ is broadly framed (Purtova, 2018), while

non-personal data remains undefined (Verma and Gurtoo, 2021). Moreover, uncertainty exists regarding the possibility of owning personal data (Asswad and Gómez, 2021). The dynamic nature of the concept is evident, as data not presently deemed personal could attain that status if it could potentially identify an individual (Sivarajah et al., 2017). Evolving technology further complicates matters, with machine-generated data possibly becoming personal data in specific contexts (Kamarinou et al., 2016). As the debate around data ownership is held in steady progress, it is pertinent to investigate the same in the digital society in India.

Studies that examine surveillance capitalism and the appropriation of behavioural data (Paunksnis, 2023); narratives persuading people migrate to digital payments during the Digital India campaign (Sam et al., 2023); the consequences of digital technologies on cultural and creative industries (Bouquillion, and Ithurbide, 2023); digital empowerment (Ashok, 2022); and the cultural and social contexts surrounding the establishment of a cashless economy (Athique, 2019) deals with a multitude of issues pertaining to digitalisation initiatives. Some works like privacy and data protection (Singh, 2011; Bais, 2021) emphasised the impotence of legal measures for protection of privacy. Scholarly works do exist that forecast potential impediments posed by social and cultural contexts in India to the successful realisation of digitisation initiatives. These works examine issues such as the use of digital identity for government services through Aadhaar (Mir, 2020a); exclusion of individuals from digitisation efforts, leading to the deprivation of entitled services (Mir et al., 2020b); obstacles faced in achieving a smart village through digitalisation due to the digital divide and cultural factors (Malik et al., 2022); and social inequalities and digitalisation (Tewathia et al., 2020).

Certain studies argue that the Digital India campaign has resulted in the commercialisation of bias, leading to disparate outcomes for marginalised and structurally oppressed classes (Ghosh, 2021). The rise of surveillance capitalism through the Digital India campaign, encompassing the collection of users' behavioural data, has also been well-documented (Šarūnas, 2023). The Digital India campaign has also been viewed as a state-led surveillance project (Abraham, 2019). The phenomenon of platform capitalism in India has also been subject to scholarly investigation (Athique, 2020), along with concerns related to the use of facial recognition for boarding pass verification in Indian airports through the DigiYatra initiative (Awtaney, 2019). Some studies argue that the advent of smart citizenship and the digital shift has perpetuated historical, social disparities from the urban realm to the digital domain (Datta, 2018). Furthermore, it has been recognised that the magnitude of inequalities at different geographic locations significantly affects the utilisation of digital technology (Venkataramanan et al., 2021). A caste-based digital divide has also been identified (Rajam et al., 2021).

In social media consumption, several studies have investigated the impact of social and cultural factors on the subscription to over-the-top (OTT) video streaming services in India (Nagaraj et al., 2021). Moreover, extensive research has been dedicated to regulating cultural and creative industries through digital policies and their implications in the Digital India campaign (Ithurbide et al., 2023; Bouquillion and Ithurbide, 2023). The absence of a comprehensive digitalisation policy guiding initiatives and program implementation across various Indian states has been emphasised (Bera, 2019).

In India, scholarship on digital society and its various manifestations are on secular growth but one serious lacunae found in the literature survey is the literature gap in the scholarship that systematically tackle data governance through proper perspective. Scholarship on data rights and data trust is still in its nascent stage. During India's digital

transformation, a noticeable scarcity of robust scholarly investigations into the societal implications of data governance is apparent. This search caters to the literature gap in data governance debates.

3 Research methodology

3.1 Research questions

This study is guided by the following research questions:

- **RQ 3.1.1:** What legal frameworks for data protection incorporate safeguards for personal data through legislative measures in different countries?
- **RQ 3.1.2:** What policy drafts in India address the notion of data rights, and how comprehensively do these policies cover the spectrum of data protection?
- **RQ 3.1.3:** To what extent do data rights protection provisions within different Indian data policies consider the interplay between data rights and India's social structure?
- **RQ 3.1.4:** Is the data rights and data trust approach to data governance in India adequate given the country's socio-cultural and legal context?

3.2 Research design

This study employs a mixed-methods approach, integrating both qualitative and quantitative research techniques to ensure a comprehensive understanding of data rights and fiduciary responsibilities in the Indian context.

- **Research approach:** The study adopts a deductive approach, beginning with classical theories of rights, property ownership, and fiduciary principles. These theoretical foundations are examined in relation to algorithm-driven social environments and tested against contemporary data protection frameworks. The study evaluates the applicability of these theories within India's unique socio-cultural structure.
- **Comparative analysis:** A cross-jurisdictional analysis of data protection policies and AI governance frameworks is conducted to highlight best practices and contextual differences. The Justice B.N. Srikrishna Committee Report (JBNSCR, 2018) and the Digital Personal Data Protection Act (DPDPA, 2023) are benchmarked against global frameworks to assess their alignment with fiduciary trust principles.

3.3 Data collection

- **Primary data**
 - Textual analysis of original legal and policy documents related to data protection across India and other jurisdictions.

- A historical review of classical legal-philosophical literature, including Hobbes, Locke, Rousseau, and Thomas Paine, to trace the evolution of rights and fiduciary responsibilities.
- In-depth interviews with policymakers, legal experts, and stakeholders from the data governance ecosystem. Publicly available interview transcripts from media sources, panel discussions, and regulatory bodies will supplement primary data.
- **Secondary data**
 - A review of existing literature, legal reports, and government documents on data protection, fiduciary obligations, and structural inequalities in India.
 - Analysis of algorithmic governance and its social implications from academic journals, think-tank reports, and industry white papers.

3.4 *Data analysis*

- **Qualitative analysis**
 - Thematic analysis of legal texts and policy documents to identify patterns in data rights protection and fiduciary trust frameworks.
 - Coding and categorisation of interview transcripts to discern key concerns regarding data protection, fiduciary obligations, and social structures.
- **Quantitative analysis**
 - Descriptive statistical analysis to assess the frequency, trends, and coverage of data protection provisions in legal and policy documents.
 - Comparative content analysis of international data protection frameworks with India's DPDPA 2023 to evaluate convergence and divergence in fiduciary principles.

3.5 *Comparative analysis*

- **Benchmarking fiduciary trust:** Examining fiduciary principles outlined in Indian policies (e.g., JBNSCR, 2018; DPDPA, 2023) against traditional trust models in Indian society (e.g., community-driven data governance and informal trust networks).
- **Structural oppression and data rights:** Investigating the intersection of data rights with caste, gender, and economic hierarchies, to assess whether existing legal frameworks adequately protect marginalised communities.

3.6 *Result and discussion*

- **Feasibility of fiduciary principles:** Synthesising survey responses, legal text analyses, and interview data to evaluate whether Indian policies adequately enforce fiduciary responsibilities.

- **Effectiveness of Indian Data Protection Laws:** Assessing whether the DPDPA 2023 sufficiently addresses structural inequalities in data governance.

4 Data protection in the west

Data protection in the Western context encompasses the legal and ethical principles governing personal data collection and usage and protecting users' interests. Key facets encompass stringent privacy laws epitomised by the European Union's General Data Protection Regulation (GDPR), which affords individuals the rights to data access, awareness, and deletion. Emphasis on informed and explicit consent principles underscores data protection, while notions of data ownership grant individuals control over their data. Data portability, the right to erasure, and transparency further bolster data protection. Accountability and enforcement mechanisms are central pillars of data protection, as data controllers must ensure compliance with privacy rules and fortify data security to thwart breaches. Regulation of cross-border data flow, consistent protection, and ethical considerations encompassing fairness and societal welfare shape Western data rights discussions. Table 1 represents a survey of legal protection of data in select countries of the world.

The data protection frameworks have implications for data rights. Each framework grants individuals certain rights over their data and imposes obligations on organisations that handle this data, promoting greater transparency, control, and accountability. Each country adopts systematic approach to protect the data rights of their citizens. This approach seems more or less oriented to their national dynamics, culture and national philosophy. Citizen's right over their personal data is paramount concern in EU [Row 1, Column 5]. The GDPR also upholds obligation of proprietary owners to seek consent from users for data processing [Column 5, Row 1]. Some countries are particular about the right of the citizen to know what personal data is collected by a data vendor [Row 2, Column 5]. Even businesses are encouraged to respect user preferences [Row 2, Column 6]. In USA, the idea of upholding the basic values of the American society is held high through broad policy directives [Row 2, Column 5]. In UK citizens' right over their personal data is protected [Row 3, Column 5] and the same is protected in Singapore [Row 4, Column 5]. Data right is facilitated through individual control over personal data in Australia [Row 6, Column 6]. In Brazil citizen right to anonymise their data is protected [Row 7, Column 5]. A review of the data regimes gives cue to the concerns raised by national governments over the misuse of citizen data by data vendors or proprietary platforms (Table 1). Most countries listed in the table underlines right such as seeking consent, right to know which data is collected, data rights linked with societal values, individual control over their personal data, right of citizens to anonymise their data, the legal frameworks have created broad parameters to protect individual data right. This point towards increasing preoccupation of national societies in viewing data as a right, a product of the individual and commitment of government to protect the data as right. The significant patterns evident in Table 1 revolve around the following key themes:

Table 1 Laws and data rights in select countries

<i>S. no</i>	<i>Country</i>	<i>Legal and policy name</i>	<i>Year of passing</i>	<i>User data ownership and rights provision</i>	<i>Implications for protection of rights</i>
1	EU	General Data Protection Regulation (GDPR, 2018)	2018	GDPR grants individuals the right to own and control their personal data. It allows users to access, correct, and delete their data, as well as the right to data portability, enabling users to transfer data between services. Additionally, GDPR mandates data processors to obtain explicit consent for data processing and imposes strict penalties for data breaches	Data right is promoted through increased transparency, consent, and accountability. Users have greater control over their data, reducing the risk of unauthorised use and fostering trust in digital services
2	USA	California Consumer Privacy Act (CCPA)	2018	CCPA gives Californian residents the right to know what personal data is being collected and shared, and the right to opt-out of data selling. It allows users to delete their data and prohibits discrimination against those exercising their privacy rights	Data right is encouraged by providing consumers with more control over their data and increasing transparency in data handling practices. Businesses are incentivised to respect user preferences and avoid unfair practices
		Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People (AIBR, 2022)	2022	The Blueprint for an AI Bill of Rights is a set of five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the rights of the American public in the age of artificial intelligence	These principles are a blueprint for building and deploying automated systems that are aligned with democratic values and protect civil rights, civil liberties, and privacy. This framework applies to (1) automated systems that (2) have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services
3	UK	Data Protection Act 2018	2018	The Data Protection Act enforces data protection principles similar to GDPR, providing users with rights over their data. It also has provisions to protect against unlawful data processing and data breaches	Data right is promoted by safeguarding personal information and giving individuals the power to manage how their data is used, leading to greater trust in the digital ecosystem and encouraging responsible data practices

Table 1 Laws and data rights in select countries (continued)

<i>S. no</i>	<i>Country</i>	<i>Legal and policy name</i>	<i>Year of passing</i>	<i>User data ownership and rights provision</i>	<i>Implications for protection of rights</i>
4	Singapore	Personal Data Protection Act (PDPA)	2012	PDPA governs the collection, use, and disclosure of personal data. It allows individuals to access, correct, and withdraw consent for data use. Organisations must inform users about data practices and obtain consent before processing data	Data right is supported through user consent and informed decision-making. Users are empowered to manage their data, enhancing accountability and fostering a culture of responsible data handling by organisations
5	Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	2000	The PIPEDA regulates the private sector's collection and use of personal data. It grants individuals the right to access their data, challenge its accuracy, and file complaints against non-compliant organisations	Data right is advanced through increased accountability for businesses handling personal data. Individuals have recourse if their data rights are violated, fostering trust in data-driven services and encouraging organisations to adopt privacy-conscious practices
6	Australia	Privacy Act 1988	1988	The Privacy Act provides guidelines for handling personal information. It allows individuals to access and correct their data, opt-out of direct marketing, and protects sensitive information	Data right is facilitated through individual control over personal data, and the Act encourages organisations to maintain data accuracy and transparency, promoting ethical data usage and building trust with consumers
7	Brazil	General Data Protection Law (LGPD)	2018	LGPD grants users the right to access, delete, and anonymise their data. It requires organisations to obtain explicit consent for data processing and includes provisions for data protection and breach notification	Data right is reinforced by giving users control over their data and ensuring organisations prioritise data security. The law also holds companies accountable for their data practices, fostering trust among consumers and promoting ethical data handling
8	Other	Various Data Protection Laws	–	Many countries have their own data protection laws, such as Japan's Act on Protection of Personal Information, South Korea's Personal Information Protection Act, and India's Personal Data Protection Bill. These laws often grant individuals similar rights over their data and impose obligations on data controllers and processors	Data right is strengthened worldwide through international recognition of data rights and responsible data handling practices. The protection of user data becomes a global priority, promoting trust and transparency in the digital world

The inputs are selected through a rigorous analysis of laws in respective countries to protect data right.

Source: Authors

4.1 User control and rights

Across various data protection frameworks, a consistent pattern emphasises granting individuals control over their data. This includes rights such as access, correction, deletion, and data portability. These rights empower individuals to manage their information, promoting a sense of ownership and control over their digital identity.

4.2 Transparency and accountability

Many frameworks underscore the importance of transparency in data practices. They mandate explicit consent for data processing, and organisations must inform users how their data will be used. This transparency increases accountability, as users are informed participants in the data exchange.

4.3 Ethical use of data

The frameworks collectively contribute to ethical living by advocating for responsible data handling. Users are given the ability to make informed decisions about how their data is used, and organisations are obligated to handle data in ways that respect user preferences and rights.

4.4 Trust and confidence building

By providing individuals with greater control, transparency, and accountability, these frameworks build trust between users and the digital services they engage with. Trust is a cornerstone of ethical living in the digital age, as users need to feel confident that their data is being handled appropriately.

4.5 Global implications

While each framework is specific to a particular region or country, the frameworks surveyed also refers to the existence of similar data protection laws in several other countries, such as Japan, South Korea, and India. This highlights a global trend toward recognising the importance of data rights and responsible data handling, underscoring the importance of these principles on a broader scale.

4.6 Technology-specific considerations

The mention of the “Blueprint for an AI Bill of Rights” emphasises the need to extend data protection principles to emerging technologies like artificial intelligence. This shows that ethical living extends beyond traditional data protection to encompass new and evolving technological domains.

4.7 Legal and policy evolution

Newer laws like the California Consumer Privacy Act (CCPA) and the Blueprint for an AI Bill of Rights (AIBR) demonstrate a dynamic legal landscape responsive to technological advancements and evolving societal expectations.

5 Data rights, data policy and Indian approach

In July 2018, a panel of experts appointed by the Indian Government released a preliminary version of the Personal Data Protection Bill (PDPB, 2018) and an extensive report outlining the committee's recommendations and rationale for the bill's provisions (JBNSCR, 2018). India's data protection legislation primarily consists of confidentiality requirements and regulations outlined in the Information Technology Act of 2000 (ITR, 2011). These regulations have faced criticism since their inception and, despite being in place for several years, have yet to be effectively enforced. Consequently, the PDP Bill, which draws substantial inspiration from the Indian Supreme Court's landmark ruling affirming the fundamental right to privacy (Supreme Court of India, 2017), represents a positive addition to the discourse on privacy and data protection.

The accompanying report, titled "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" (JBNSCR, 2018), explores various global approaches to privacy law and regulation, broadly categorising them into three models influenced by the European Union, USA, and China. The committee underscores that the report's primary goal and the PDP Bill is to forge a unique path for data protection in India. This path could potentially serve as a model for other nations in the Global South. In the process, the committee embraces a concept borrowed from American scholars, which regards data controllers or processors as 'fiduciaries' (Balkin, 2015). However, the report has limited discussion about whether such a model suits the Indian context and whether various policy drafts effectively address the challenges individuals face due to social structures.

Table 2 presents the evolution of a comprehensive framework in India that addresses issues related to data rights, data protection, data ownership, privacy, and other matters encompassed by the broader data rights debate.

Table 2 provides insights into India's various data related enactments and reports, focusing on their implications for data rights and ownership.

5.1 *Identification of key documents*

The table identifies and summarises key AI-related documents and reports in India. The documents represent the regulatory landscape dealing with data rights and ownership.

5.2 *Provisions for data rights*

The table highlights whether each document includes provisions explicitly related to data rights. This information is crucial for assessing how these regulations address individuals' rights over their data.

5.3 *Social structure consideration*

The table discusses whether the documents consider India's social structure while addressing data rights and ownership. This aspect is important because rights and access to data can vary based on an individual's position in society.

Table 2 Data rights and AI/Data policy landscape in India

<i>S. no</i>	<i>AI Enactment</i>	<i>Year</i>	<i>Core contents</i>	<i>Purpose</i>	<i>Provisions for data rights</i>	<i>Whether specific provisions to deal with data rights and social structure in India</i>
1	Principles for Responsible AI (PRAI, 2021)	2021	Set of principles for the development and use of AI in India	To ensure AI is developed and used responsibly that provides for a framework for designing AI which ensures fundamental rights guaranteed under the Constitution	There are severe social costs of incorrect decisions by automated systems, such as loss of fundamental rights due to incorrect decisions in services offered by the state and in criminal identification systems (p.16), and infringement of right to privacy when entities may use personal data without the explicit consent of concerned persons (p.22). Chapter titled 'Principles for Responsible Management of AI Systems' extensively discusses role of various stakeholders such as government, citizens, regulators, private sectors, research community, standard setting bodies, security auditors in instituting responsible management of AI in India that could protect rights of citizens (p.38). The draft talks about Constitutional morality (pp.38–39), which indirectly refers to the policies framed by government to uphold constitutional morality over social morality thereby protecting various rights specified in Part III of the Indian Constitution such as right to equality, (A–14), right against discrimination (A–15 & 16), right to life and healthcare (A–21) right to privacy (A–21) (pp.38–40). The principles for responsible management of AI may be derived from the Constitution and all the laws enacted under it (p.40). The draft proposes principles for designing AI that enables fundamental right (p.40)	The draft talks extensively about rights under the constitution and the protection of same under AI systems. But the document fails to spot the data right or users' right to possess and protect the right to user data they generate

Table 2 Data rights and AI/Data policy landscape in India (continued)

<i>S. no</i>	<i>AI Enactment</i>	<i>Year</i>	<i>Core contents</i>	<i>Purpose</i>	<i>Provisions for data rights</i>	<i>Whether specific provisions to deal with data rights and social structure in India</i>
2	Justice B.N. Srikrishna Committee Report (JBNSCR, 2018)	2018	Framework for data protection in India	To ensure personal data of individuals is protected	Proposes notions such as data principals and data fiduciary (p.7) and upholds the notion that in a digital economy an individual who creates data and allows an entity to process such data of a user must be transacted in notion of trust which is the basis of fiduciary trust	The draft fails to note that in India rights are closely linked with ones location in the social structure. Such as scenario requires special care to rights in digital economy where notion of rights freedom and individual identity are closely connected with who owns proprietary platforms and which individual uses if for what purposes on whose platforms
3	The Draft of Personal Data Protection Bill 2018 (DPDPB, 2018)	2018	Comprehensive legislation for the protection of personal data	To regulate the use of personal data by businesses and government	Provisions for user consent, data localisation, data transfer, and the establishment of a data protection authority. Notions such as data, data principal, data fiduciary, are defined (p.3). Data related harm is defined (p.4). Provides provisions for Processing of personal data on the basis of consent, and other context of processing of data (p.9), rights of data principals are clearly mentioned (p.14),	The draft bill however, failed to mention the data rights in terms of structural oppression In India which requires to be considered as important criteria of data ownership debates

Table 2 Data rights and AI/Data policy landscape in India (continued)

<i>S. no</i>	<i>AI Enactment</i>	<i>Year</i>	<i>Core contents</i>	<i>Purpose</i>	<i>Provisions for data rights</i>	<i>Whether specific provisions to deal with data rights and social structure in India</i>
4	India Data Accessibility Background Note and Use Policy (IDABNUP, 2022)	2022	Framework for ensuring accessibility and use of public data	To provide a policy framework for making public data accessible	Addresses challenges with open data sharing and use. Digitalisation has increased the volume of data which also created problem of leaks, algorithm bias, cyber attacks, necessitating a data governance inevitable (p.2). Facilitate a robust data governance strategy (p.7) Open data accordingly, is perceived with a degree of suspicion, not only because of the propensity it creates for accountability but also for the lack of understanding around misuse of data and safeguards against it (p.7)	There is no robust attention being given to the correlation between social structure in India and open data. So rights aren't core concern in the draft
5	India Data Accessibility and Use Policy (IDAUP, 2022)	2022	Policy for sharing and use of government data	To provide guidelines for government agencies to share and use data for public welfare	No specific provision for data rights. Transform India's ability to harness public sector data for facilitating social transformation. Any data sharing shall happen within legal framework in India, its national policies and legislation (p.2). Ethical sharing data is core concern	No reference to data rights and India's unique society and its broad context in which rights are violated

Table 2 Data rights and AI/Data policy landscape in India (continued)

<i>S. no</i>	<i>AI Enactment</i>	<i>Year</i>	<i>Core contents</i>	<i>Purpose</i>	<i>Provisions for data rights</i>	<i>Whether specific provisions to deal with data rights and social structure in India</i>
6	The Report of the Artificial Intelligence Task Force (RAITF, 2018)	2018	Recommendations for the development and adoption of AI in India	To provide a roadmap for the development and adoption of AI in India	The Report on the Artificial Intelligence Task Force, RAITF 2018, constituted by the Ministry of Commerce and Industry, identifies 10 domains of relevance for India, FinTech, healthcare, education, environment, agriculture and food processing, and manufacturing. The report examines the application of AI in key sectors identified and investigates the future role of AI in India. The report emphasises the responsible use of AI, which may otherwise cause serious harm. One important recommendation of the government report is fostering interdisciplinary research, including humanities, social sciences, law, science, medicine and engineering, to facilitate a deeper understanding of AI-based technologies' possibilities (see p.48)	No specific provision for data rights
7	NITI Aayog Discussion Paper National Strategy for Artificial Intelligence (NSAI, 2018)	2018	Framework for the development of AI in India	how India can leverage the transformative technologies to ensure social and inclusive growth in line with the development philosophy of the government (p.5)	It provides recommendations to protect intellectual property rights (p.48), refers to Supreme Court of India verdict terming privacy as a fundamental right, making citizens aware of their privacy and educate them about how to protect it not only by state enforcement agencies, revising curriculum structure at pan India level to educate young people about privacy rights (p.88), calls for a instituting a data privacy legal framework which creates data protection framework which protects data as a human rights (p.93)	1, There is no reference to specific data rights, data ownership, and data as property rights 2, There is a blatant neglect of data ownership rights in particular there is no reference to the matters such as users generate so much user data which requires to be discussed as a property of the users and the use of third party without the knowledge of the creator amounts to be a

Table 2 Data rights and AI/Data policy landscape in India (continued)

<i>S. no</i>	<i>AI Enactment</i>	<i>Year</i>	<i>Core contents</i>	<i>Purpose</i>	<i>Provisions for data rights</i>	<i>Whether specific provisions to deal with data rights and social structure in India</i>
8	Joint Parliamentary Committee Report on the Personal Data Protection Bill, 2019 (JPCR, 2021)	2021	Recommendations for amendments to the Personal Data Protection Bill 2019	To address concerns raised by stakeholders and ensure effective data protection	Underscores the core significance of data in 21st century. It understands that We are heading towards a data and technology driven 'Web of the World' (p.1) and considers data is vital for transforming India through digital economy. Viewing data as a new asset, the committee considers that protecting data is vital (p.4). The committee considers that its difficult to distinguish between personal data and non-persona data when data is massively collected and transferred (p.23). Committee also recommends that no social media platform should be allowed to operate in India unless the parent company handling the technology sets up an office in India. (p.34)	The committee report is silent about the interplay between data and rights structured by social structures in India

Table 2 Data rights and AI/Data policy landscape in India (continued)

<i>S. no</i>	<i>AI Enactment</i>	<i>Year</i>	<i>Core contents</i>	<i>Purpose</i>	<i>Provisions for data rights</i>	<i>Whether specific provisions to deal with data rights and social structure in India</i>
9	The Personal Data Protection Bill, 2019 (PDPB, 2019)	2019	Comprehensive legislation for the protection of personal data	To provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India	It defines data (p.3), harm (p.3), personal data (p.4), obligations of data fiduciary (p.6), grounds for processing personal data (p.8), and rights of data principal (pp.10–13)	The PDPB 2019 however fails to make note of the interplay between India's social structure and data rights of Individuals

Table 2 Data rights and AI/Data policy landscape in India (continued)

<i>S. no</i>	<i>AI Enactment</i>	<i>Year</i>	<i>Core contents</i>	<i>Purpose</i>	<i>Provisions for data rights</i>	<i>Whether specific provisions to deal with data rights and social structure in India</i>
10	The Digital Personal Data Protection Bill, 2022 (DPDPB, 2022)	2022	Comprehensive legislation for the protection of personal data in digital spaces	It provides for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process personal data for lawful purposes	The bill defines 'automated' means any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data (p.2). It also defines 'data' means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means (p.3). It defines 'personal data' as any data about an individual who is identifiable by or in relation to such data (p.4). Data fiduciary is obliged to process personal data of data principals only according to the rules specified in the act (p.6). It specifies various scenarios of data breach, consent, and other occasions in which data can be manipulated or processed by fiduciary and provides for protection of data breaches. Rights and duties of data principals are extensively discussed in Chapter 3 (pp.14–15)	Bill fails to look at the social structure in India to deal with persona data protection and data rights
11	The Digital Personal Data Protection Act (DPDPA, 2023)	2023	Comprehensive legislation for the protection of personal data in digital spaces	Provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes	Some additions have incorporated to DPDPB 2022 such as person also includes a reference to Hindu Undivided family. Exemptions to data processing by the State on grounds such as national security may lead to data collection, processing, and retention	

Source: Authors

5.4 *Gaps and limitations*

The table reveals areas where regulations fall short in addressing data rights and ownership comprehensively by pointing out the gaps and limitations in each document. These gaps provide insights into potential areas for improvement and further legislative development.

5.5 *Evolution over time*

The chronological arrangement of the documents allows for tracking the evolution of regulatory efforts related to data rights and ownership in India. This historical perspective helps make sense of the progression of ideas and policies in this domain.

5.6 *Intersection of AI and data rights*

The table shows how AI technologies intersect with data rights and ownership. It provides instances where AI-based decision-making can impact fundamental rights and personal data protection.

5.7 *Policy focus*

For documents that focus on broader AI development strategies, the table highlights whether data rights and ownership are given due attention within these strategies. This insight is essential for understanding the overall policy landscape.

5.8 *Recommendations and omissions*

The table highlights specific recommendations made within these documents and the areas they omit. The table particularly draws attention to the lacunae in policy drafts addressing social structures and their linkages with data rights. This information can guide policymakers, researchers, and advocates in strengthening future regulations.

Table 2 provides a consolidated view of how different AI enactments and reports in India address data rights and ownership concerns while highlighting areas requiring further attention. The most important among them were JBNSCR 2018 and PDPB 2019.

JBNSCR (2018) presents a comprehensive blueprint for India's approach to data rights. It says that "it is our view that any regime serious about safeguarding personal data of the individual must aspire to the common public good of both a free and fair digital economy" (p.7). It further says, "Freedom refers to enhancing the autonomy of the individuals with regard to their personal data in deciding its processing, which would lead to an ease of flow of personal data" (p.7). The report views that "Fairness pertains to developing a regulatory framework where the rights of the individual with respect to her personal data are respected, and the existing inequality in bargaining power between individuals and entities that process such personal data is mitigated" (p.8). The report proposed neologism to deal with data rights, saying, "In such a framework, the individual must be the 'data principal' since she is the focal actor in the digital economy. The relationship between the individual and entities with whom the individual shares her personal data is one that is based on a fundamental expectation of trust.

Notwithstanding any contractual relationship, an individual expects that her personal data will be used fairly in a manner that fulfils her interest and is reasonably foreseeable. This is the hallmark of a fiduciary relationship” (p.27). The report continues by saying, “In the digital economy, depending on the nature of shared data, the purpose of such sharing and the entities with which sharing happens, data principals expect varying levels of trust and loyalty. For entities, this translates to a duty of care to deal with such data fairly and responsibly for purposes reasonably expected by the principals. This makes such entities data fiduciaries” (p.8).

Further to this, report notes that “Data fiduciaries must only be allowed to share and use personal data to fulfil the expectations of the data principal in a manner that furthers the common public good of a free and fair digital economy. It is our view that a regime based on the abovementioned principles and implemented through the relations described above will ensure individual autonomy and make available the benefits of data flows to the economy” (p.8). “In our view, ensuring the protection of personal data and facilitating the growth of the digital economy are not in conflict and has rightly been pointed out, serve a common constitutional objective” (p.8). Rights (of which the right to privacy is an example) are not deontological categories that protect the interests of atomised individuals; on the contrary, they are tools that, as Raz points out, are necessary to realise certain common goods. The importance of a right in this account is not because of the benefit that accrues to the rights holder but instead because that benefit is a public good that society as a whole enjoys. This is a critical distinction and often missed in simplistic individual-centric accounts of rights. (p.9). Thus, the construction of a right itself is not because it translates into an individual good, be it autonomy, speech, etc., but because such good creates a collective culture where specific reasons for state action are unacceptable. In the context of personal data collection, use and sharing in the digital economy, it is our view that protecting an individual’s autonomy is critical not simply for her own sake but because such autonomy is constitutive of the common good of a free and fair digital economy. Such an economy envisages a polity where the individual is autonomously deciding what to do with her personal data, entities are responsibly sharing such data, and everyone is using data, which has immense potential for empowerment in a manner that promotes overall welfare (p.9). The JBNSCR and PDPB presented a comprehensive framework for data protection, which presented a debate about the appropriateness of data trust and rights to the Indian situation.

6 Data trust vs. data rights

A data trust, as delineated by various scholars (Hardinges, 2018; Hardinges and Wells, 2018; Delacroix and Lawrence, 2019; Bunting and Lansdell, 2019), involves an entity entrusted with securely holding data on behalf of beneficiaries. Its structure is adaptable, contingent on the specific context (Manohar, 2020), and this concept carries significant global implications (Fadler, and Legner, 2022). Given that dominant data players often reside in economically robust regions, the priorities of local data protection diverge significantly from those of foreign nations. Social diversity inevitably impacts data trusts, which function as custodians safeguarding user data. This concept operates on the legal principle of a trust, where an entity manages something for the benefit of a third party or a defined purpose. In the data realm, this trust protects user interests and oversees data

management (BPE Solicitors, 2019). For example, when data is shared with a third party, a data trust ensures encryption and adherence to policies (Paprica et al., 2020).

However, a conspicuous issue in India is the absence of trust within the social fabric, where different social groups are starkly polarised along the lines of caste, religion, and region, subsequently impacting trust principles. Lower caste individuals often lack trust in upper castes, and vice versa (Ambedkar, 1990; Rodriguez, 2011), and similar trust deficits manifest between genders within society (Amutha, 2017). Nonetheless, the Indian constitution was designed to transcend these societal barriers (Ahmad, 2017; Saracini and Shanmugavelan, 2019). Therefore, the effectiveness of data policies in addressing trust deficits unique to Indian society must be firmly anchored in the Constitutional philosophy, and these policies correspond to them (Biju and Gayathri, 2023).

It raises the crucial question: Is the concept of data trust suitable for the densely divided social landscape in India? To ascertain its applicability, a thorough examination of its principles is imperative. Trusts typically involve the transfer of property title to a trustee who must fulfil obligations for the benefit of the beneficiary (Clarry, 2014). Applied to data, this translates to viewing data as property, users as beneficiaries, and the entity as a trustee. Interestingly, a legal report by the Open Data Institute (Pinsent Masons and Ors., 2019) argues against trusts being suitable for managing user data. So, why has the concept of data trust gained traction?

The trust principles envisioned for data protection through a fiduciary relationship can be likened to feudal land relationships, where tenants till land owned by landlords. The tenant receives a piece of land for cultivation, and the proceeds are ostensibly their own. However, whatever the tenant produces often goes to the landlord. Similarly, data platforms figure out data lords and users as tenants whose labour is placed under the auspices of data lords. Applying the trust format to protect the interests of data tenants can inherently conflict with the interests of data lords, creating a conspicuous absence of trust in the relationship that resembles feudal servitude.

In India, the Personal Data Protection Bill (PDPB, 2019) and the Non-Personal Data Report (MeitY, ND) make mention of data trust. The fiduciary trust concept was initially introduced in the JBNSCR 2018. These regulations and reports aim to safeguard users through rules or comprehensive laws governing data handling. However, these rules are limited in scope as they fail to account for the complex web of trust dynamics among various caste and social groups in India. Table 2 provides a detailed analysis of policy drafts and bills related to data protection. However, it becomes evident that the trust principles do not adequately address caste-based conflicts and other forms of enmity in India, which the introduction of data trust concepts might exacerbate. While the Indian constitution strives to overcome these difficulties by incorporating provisions for underprivileged groups, data protection policies seem to have inadequately addressed these issues in their efforts to protect individual data.

The role of a data trust as an oversight body for data sharing and usage practices, acting as an intermediary to enforce ethical data use, is affected by these entities' social composition, operational philosophy, and commitment to embracing the inclusive principles embedded in the Indian constitution. Their responsibilities include taking direct action against violations, such as issuing public notices and terminating data access (BPE Solicitors, 2019), but these actions may be fraught with conceptual inaccuracies.

To fulfil its oversight role, a data trust derives authority from users, which authorities could establish through user collectives, contracts, or appointments. However, the

systematic integration of these authorities in accordance with India's unique social context is essential. The structure and practices of a data trust may vary based on the data's purpose and sensitivity; public data vs. personally identifiable data, for instance, require different levels of scrutiny. A critical factor here is the entity's role in managing data usage, representing users and data providers, and ensuring compliance with stated purposes.

Currently, data sharing chains established through data trust principles lack adequate user representation, social diversity, and inclusive philosophy, which complicates the existence of data trusts and may favour third parties that assume the role of data lords. This emphasises the need for increased trust and accountability, with data trusts having to establish trust among stakeholders through effective accountability mechanisms. However, trust is a scarcer commodity in the Indian social system (Delacroix and Lawrence, 2019).

Furthermore, the question arises: Does the property-led data control model have relevance in addressing data violations and social structures in India? Current data governance models (e.g., GDPR 2018 and AIBR 2022, as seen in Table 1) grant operational authority to data processors, but their actions are limited by granting individuals rights to data ownership. These rights constrain the mismanagement, manipulation, and appropriation of data tenants by data lords. The approach, developed through the concept of rights to safeguard individual interests in data, is analogous to property rights (Victor, 2013). This approach results in individuals possessing inherent and non-transferable rights over their personal data (Schwartz, 2004). Consequently, third-party access to data must adhere to terms agreed upon by individuals, with limitations similar to property arrangements.

However, the property ownership rights approach to data protection poses significant challenges in India, where discussions of data rights must consider the social context. In cases where data is accessed without user consent by a third party, the question of who accesses whose data becomes paramount in India (Balkin, 2018). This leads to addressing data protection through fiduciary trust and responsibilities, which promote the concept of fiduciary obligations (Balkin, 2016). Fiduciary duty compels data processors to act ethically in the interests of users. Nevertheless, it remains uncertain whether trust principles can effectively surmount age-old social divides in India, which the introduction of data trust principles may further entrench.

7 Social divides, trust law and data fiduciary

Labels such as 'trust' and 'fiduciary,' used in the PDPB and the GDPR context, may be considered incongruent with the social system in India, where different social groups have poor inter-group trust and power dynamics. The practical application of fiduciary duties and trusteeship to ensure data processors' protection of user interests is more likely to be flawed in countries like India (Bailey and Goyal, 2019). When viewed from a valid perspective, the system of notice and consent is often inadequate in preventing data misuse. This inadequacy has led to solutions such as Data Trusts, which are founded on fiduciary principles. Nevertheless, the data in Table 2 reveals the absence of a comprehensive fiduciary framework within Indian laws. Instead, legal frameworks rely on notice requirements, processing restrictions, and consent regulations to safeguard user interests from data processors (Balkin, 2016).

The information fiduciary approach disregards the inherent conflict of interests between users and data processors within India's socially divided and polarised landscape. Fiduciaries acting in users' best interests are at odds with their business models, which often resist granting users control over data sharing. This contradiction is deeply rooted in Indian society. The fiduciary framework cannot challenge discrimination and social dynamics of caste, gender and other social polarisation in India; the regulation of practices that encroach upon user rights and interests by the fiduciary framework is not the surety (Pozen and Khan, 2019; Bailey and Goyal, 2019; Balkin, 2016; Whitt, 2020; McDonald, 2019). The conflict of interests inherent in trust principles is exacerbated by deep-seated social divisions, such as caste divides and gender discrimination. Many legal and constitutional principles aim to address these societal tensions. Table 3 presents a list of such provisions. However, the fundamental question remains whether subsequent policy interventions align with the principles envisioned for addressing social disparities. For this to materialise, the data protection frameworks must anchor on constitutional principles, thereby sourcing the strength it requires to overcome social dynamics.

Table 3 Legal protection against various forms of structural oppression in India

<i>Serial number</i>	<i>Full name of the act</i>	<i>Year of passing</i>	<i>Major provisions for protection of rights of Indians</i>	<i>Guarantees provided</i>	<i>Effectiveness in India</i>
1	Constitution of India	1950	Article 14: Right to Equality	Prohibits discrimination and ensures equal protection	Provides a fundamental right against discrimination, but implementation challenges persist
			Article 15: Prohibition of Discrimination	Prevents discrimination based on religion, race, caste, etc.	Allows for positive discrimination in certain cases to uplift marginalised communities
			Article 17: Abolition of Untouchability	Bans untouchability practices and caste-based discrimination	Criminalises practices that enforce social discrimination and promotes social inclusion
2	Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act	1989	Provides safeguards against caste-based discrimination	Establishes special courts and stringent punishments for offenses committed against marginalised communities	Provides legal protection for marginalised communities, but implementation challenges persist
3	Protection of Civil Rights Act	1955	Prohibits the preaching and practice of untouchability	Addresses discrimination and social exclusion	Aims to eradicate untouchability and caste-based discrimination

Table 3 Legal protection against various forms of structural oppression in India (continued)

<i>Serial number</i>	<i>Full name of the act</i>	<i>Year of passing</i>	<i>Major provisions for protection of rights of Indians</i>	<i>Guarantees provided</i>	<i>Effectiveness in India</i>
4	Sexual Harassment of Women at Workplace (Prevention, Prohibition, and Redressal) Act	2013	Ensures safe working environments and prevention of sexual harassment	Provides guidelines and mechanisms for addressing sexual harassment cases in the workplace	Provides legal protection for women in the workplace, but implementation challenges persist
5	Protection of Women from Domestic Violence Act	2005	Provides legal protection for women facing domestic violence	Allows for restraining orders, monetary relief, and other forms of legal recourse for victims	Provides legal protection for women facing domestic violence, but implementation challenges persist
6	Right to Education Act	2009	Provides free and compulsory education to children aged 6–14	Ensures access to education for marginalised communities	Has improved access to education for marginalised communities, but implementation challenges persist
7	National Commission for Women Act	1990	Establishes a commission to investigate and address issues facing women	Provides a platform for women's voices to be heard and for issues to be addressed	Has raised awareness of women's issues, but implementation challenges persist
8	Protection of Children from Sexual Offences Act	2012	Provides legal protection for children facing sexual abuse	Allows for stringent punishment for offenders and provides support for victims	Provides legal protection for children facing sexual abuse, but implementation challenges persist
9	Prevention of Atrocities Act	1989	Provides legal protection for marginalised communities facing discrimination and violence	Establishes special courts and stringent punishments for offenses committed against marginalised communities	Provides legal protection for marginalised communities facing discrimination and violence, but implementation challenges persist
10	National Food Security Act	2013	Provides legal entitlements for food to marginalised communities	Ensures access to food for marginalised communities	Has improved access to food for marginalised communities, but implementation challenges persist

Source: Author

The legal frameworks in Table 3 provide conditions for protecting individual rights and preventing social discrimination and other injustices in India. However, the data protection regimes and other policy interventions to protect stakeholder interests are incongruent with the legal frameworks in Table 3 to overcome social disadvantages. Frameworks in Table 2 may be insufficient in India for the following reasons:

7.1 Lack of specific provisions

The laws listed in the table do not specifically address the challenges and complexities associated with the functioning of automated decision systems using AI and ML in culturally polarised India and its social structure.

7.2 Limited scope

The laws in Table 3 primarily focus on specific aspects of discrimination and injustice in India, such as caste-based discrimination, sexual harassment, domestic violence, and protection of marginalised communities. These legal frameworks may not directly address the unique challenges posed by AI and ML systems and tends to be insufficient to deal with the structural oppression perpetuated by machine systems that may affect individual rights.

7.3 Implementation challenges

Even though the laws provide guarantees and legal protection, implementation challenges persist in India. Similar challenges can be expected in the context of AI and ML systems, where enforcing compliance and ensuring accountability can be complex.

7.4 Technological advancements

The existing laws in Table 3 may not be equipped to keep up with the pace of technological advancements and address the specific issues that arise with automated decision systems.

7.5 Ethical considerations

AI and ML systems can raise ethical concerns about transparency, explainability, fairness, and accountability. The laws in Table 3 do not explicitly address these ethical dimensions and may not provide adequate guidance on how to ensure that AI and ML systems operate in a manner that upholds principles of non-discrimination and justice, leading to the protection of user rights.

8 Result

Some key features of the Indian approach to data rights under the PDPB and PDPA 2023 included.

8.1 Data principle

The PDPB proposed establishing a data protection framework based on certain principles, including fairness, transparency, purpose limitation, data minimisation, and accountability.

8.2 Individual rights

The bill recognised certain rights for individuals, including the right to be informed, the right to access personal data, the right to correct inaccurate data, the right to be forgotten, and the right to data portability.

8.3 Consent

The bill emphasised obtaining informed and meaningful consent from individuals before processing their personal data. It proposed that consent should be freely given, specific, informed, and revocable.

8.4 Data localisation

The bill contained provisions that required sensitive personal data to be stored within India, with some exceptions. It aimed to enhance data security and sovereignty.

8.5 Data protection authority

The bill proposed the establishment of a Data Protection Authority of India (DPA) responsible for overseeing and enforcing data protection regulations.

8.6 Cross-border data transfers

The bill outlined conditions under which personal data could be transferred outside India, including the requirement of obtaining explicit consent from individuals.

While the PDPB did not directly adopt fiduciary principles, it aimed to create a robust framework for data protection, privacy, and individual rights. It must be argued that an Indian approach is yet to emerge.

9 Conclusion

In the preceding discourse and Tables 2 and 3, it has been ascertained that the legal frameworks operating within the common law jurisdiction of India lack the requisite tools to effectively address data rights issues and enforce fiduciary responsibilities related to data trust. The study's primary objective was to scrutinise the legal frameworks for data protection across various countries, encompassing safeguards for personal data through legislative measures. Table 1 comprehensively explored these legal provisions and addresses RQ3.1.1. Meanwhile, Table 2 presents the policy drafts in India that tackle the concept of data rights, evaluating the extent to which these policies encompass a comprehensive spectrum of data protection, thus addressing RQ3.1.2.

In alignment with the data policies, the research further investigated the degree to which Indian data policies consider the interplay between data rights and the intricate social fabric of India. This is elucidated within Table 2, where a separate analysis is provided to investigate how data policies correspond to the complex interconnections between data rights and their linkage with the social structure, consequently addressing RQ3.1.3.

This paper emphasises the inquiry into whether the data right and data trust approach to data governance is suitable for the Indian context. It has been determined that the principles of data trust, in the context of digital data, necessitate more refined and legally strong frameworks. It is because Indian society is shaped by a multifaceted social structure characterised by intricate and fragile trust dynamics between social groups. Concurrently, the notion of data rights remains a contentious focal point, given that Indian society is also marked by feudal-type relationships, which the constitution has endeavoured to overcome. However, the terminologies of fiduciary and principal proposed in the context of data governance find their roots in feudal social relationships, which raises the possibility of principals functioning as data tenants and fiduciaries as data lords. Therefore, without substantially altering the complex social structure in India, the data right framework may not find resonance within the Indian social milieu. This comprehensive discussion effectively addresses Research Question 3.1.4.

The conclusion of the study has several implications for policymakers, legal practitioners, and individuals concerned with data protection in India:

9.1 Policymakers

9.1.1 Reassessment of legal frameworks

The study highlights that the current legal system lacks the tools to effectively address data rights and enforce fiduciary responsibilities.

9.1.2 Consideration of social fabric

The study emphasises the need to consider the interplay between data rights and the complex social dynamics within the country. It may require a more nuanced and culturally sensitive approach to data governance.

9.1.3 Data trust frameworks

The study suggests that Indian society's trust dynamics and historical relationships may impact the implementation of data trust principles. To adopt this approach, policymakers may need to develop more refined and culturally appropriate data trust frameworks.

9.2 Legal practitioners

9.2.1 Legal adaptation

Legal practitioners should be prepared to adapt to potential changes in India's data protection laws and regulations. As the legal frameworks are reassessed and refined, legal professionals will need to stay informed about these changes and ensure compliance on behalf of their clients.

9.2.2 Cultural sensitivity

Legal practitioners should also be aware of the cultural and social nuances highlighted in the study. Understanding how data rights and trust intersect with India's unique social structure can be crucial in providing legal advice and representation related to data protection.

9.2.3 Fiduciary relationships

Legal practitioners should be cautious when applying terms like 'fiduciary' and 'principal' in data governance. The study suggests that these terms may have historical connotations that could affect how data rights are perceived and enforced. Legal professionals may need to adapt their language and strategies accordingly.

9.3 Individuals concerned with data protection:

9.3.1 Awareness and advocacy

Individuals concerned with data protection should stay informed about the evolving legal landscape in India. They can also advocate for stronger data protection measures and ensure their rights are upheld.

9.3.2 Cultural consideration

Understanding the cultural and social context of data protection in India can help individuals navigate their data rights more effectively. It may also inform their choices regarding data sharing and trust in various platforms and services.

References

- Abraham, R., Schneider, J. and vomBrocke, J. (2019) 'Data governance: a conceptual framework, structured review, and research agenda', *International Journal of Information Management*, Vol. 49, pp.424–438, <https://doi.org/10.1016/j.ijinfomgt.2019.07.008>
- Abraham, S. (2019) 'Surveillance project', in Khera, R. (Ed.): *Dissent on Aadhaar: Big Data Meets Big Brother*, Orient BlackSwan, Hyderabad, pp.111–119.
- Ahmad, N. (2017) *Racism in India: Equality Constitutionalism and Lego-Institutional Response*, SSRN: <https://ssrn.com/abstract=2903995>
- AIBR (2022) *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People*, <https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf>
- Alafaa, P. (2021) *Data Privacy and Data Protection: The Right of User's and the Responsibility of Companies in the Digital World*, SSRN: <https://ssrn.com/abstract=4005750> or <http://dx.doi.org/10.2139/ssrn.4005750>
- Alfnes, F. and Wasenden, O.C. (2022) 'Your privacy for a discount? Exploring the willingness to share personal data for personalized offers', *Telecommunications Policy*, Vol. 46, No. 7, <https://doi.org/10.1016/j.telpol.2022.102308>
- Ali, O., Shrestha, A., Soar, J. and Wamba, S.F. (2018) 'Cloud computing-enabled healthcare opportunities, issues, and applications: a systematic review', *International Journal of Information Management*, Elsevier, Vol. 43, No. C, pp.146–158.

- Al-Khouri, A.M. (2012) 'Data ownership: who owns 'My Data'?', *International Journal of Management and Information Technology*, Vol. 2, pp.1–8, <https://doi.org/10.24297/ijmit.v2i1.1406>
- Ambedkar, B.R. (1990) *Annihilation of Caste: An Undelivered Speech*, Arnold Publisher, New Delhi.
- Amutha, D. (2017) *The Roots of Gender Inequality in India*, SSRN: <https://ssrn.com/abstract=2906950> or <http://dx.doi.org/10.2139/ssrn.2906950>
- Arrieta-Ibarra, I., Goff, L., Jiménez-Hernández, D., Lanier, J. and Weyl, E.G. (2018) 'Should we treat data as labor? moving beyond 'Free'', *AEA Papers and Proceedings*, Vol. 108, pp.38–42.
- Asswad, J. and Gómez, J.M. (2021) 'Data ownership: a survey', *Information*, Vol. 12, No. 11, p.465, <https://doi.org/10.3390/info12110465>
- Athique, A. (2019) 'A great leap of faith: the cashless agenda in digital India', *New Media and Society*, Vol. 21, No. 8, pp.1697–1713, <https://doi.org/10.1177/1461444819831324>
- Athique, A. (2020) 'Digital emporiums: evolutionary pathways to platforms capitalism', in Athique, A. and Parthasarathi, V. (Eds.): *Platform Capitalism in India*, Palgrave Macmillan, Cham, pp.23–41.
- Awtaney, A. (2019) *DigiYatra: The Good and the Bad of Using your Face as a Boarding Pass for Your Flight*, CNBC TV 18, 13 September, <https://www.cnbctv18.com/views/digiyatra-the-good-and-the-bad-of-using-your-face-as-a-boarding-pass-for-your-flight-4344871.htm>
- Bailey, R., Goyal, T. (2019) *Fiduciary Relationships as a Means to Protect Privacy: Examining the Use of the Fiduciary Concept in the Draft Personal Data Protection Bill 2018*, Data Governance Network Working Paper, http://datagovernance.org/files/research/NIPFP_Rishab_Trishree_fiduciaries_-_Paper_4.pdf
- Bais, Y. (2021) 'Privacy and data protection in India: an analysis', *International Journal of Law Management and Humanities*, Vol. 4, No. 5, pp.1793–1804, <https://doi.org/10.10000/IJLMH.112146>
- Balkin, J. (2018) *Facebook and the Risks of Data Capitalism*. Yale Insights, <https://insights.som.yale.edu/insights/three-questions-prof-jack-balkin-on-facebook-and-the-risks-of-data-capitalism/>
- Balkin, J.M. (2015) *Information Fiduciaries and the First Amendment* (2015) 49 *U.C. Davis Law Review* 1183
- Balkin, J.M. (2016) 'Information fiduciaries and the first amendment', *UC Davis Law Review*, Vol. 49, No. 4, pp.1–52, https://lawreview.law.ucdavis.edu/issues/49/4/Lecture/49-4_Balkin.pdf
- Baron, J.B. (2012) 'Property as control: the case of information', *Mich Telecomm and Tech L Rev.*, Vol. 18, pp.367–418.
- Bera, S. (2019) 'Club convergence and drivers of digitalization across Indian states', *Telecommunications Policy*, Vol. 43, No. 8, p.101822, <https://doi.org/10.1016/j.telpol.2019.04.006>
- Bouquillion, P. and Ithurbide, C. (2023) 'Policy for cultural and creative industries in India: the issue of regulation through digital policy', *Contemporary South Asia*, Vol. 31, No. 2, pp.326–340, doi: 10.1080/09584935.2023.2203902.
- Boyd, D. and Crawford, K. (2012) 'Critical questions for big data', *Information, Communication and Society*, Vol. 15, No. 5, pp.662–679, <https://doi.org/10.1080/1369118X.2012.678878>
- BPE Solicitors (2019) *Extended ODI Data Trust Report: Further Use Cases to Consider*, http://theodi.org/wp-content/uploads/2019/04/BPE_PITCH_EXTENDED_ODI-FINAL.pdf
- Bunting, M. and Lansdell, S. (2019) *Designing Decision Making Processes for Data Trusts: Lessons from Three Pilots*, Office for Artificial Intelligence of the Government of the United Kingdom, <http://theodi.org/wp-content/uploads/2019/04/General-decision-making-report-Apr-19.pdf>

- Burri, M. (2017) 'The governance of data and data flows in trade agreements: the pitfalls of legal adaptation', *UC Davies Law Review*, Vol. 51, pp.65–132.
- Cadwalladr, C. and Harrison, E.G. (2018) 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', *Guardian*, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Chi, M., Huang, R. and George, J.F. (2020) 'Collaboration in demand-driven supply chain: based on a perspective of governance and IT-business strategic alignment', *International Journal of Information Management*, Vol. 52, No. C, pp.1–40, doi: <https://doi.org/10.1016/j.ijinfomgt.2019.102062>
- Clarry, D. (2014) 'Fiduciary ownership and trusts in a comparative perspective', *The International and Comparative Law Quarterly*, Vol. 63, No. 4, pp.901–933, <https://doi.org/10.1017/S0020589314000463>
- Couldry, N. and Mejias, U.A. (2019) *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*, Stanford University Press, Redwood City.
- Craglia, M., Scholten, H., Micheli, M., Hradec, J., Calzada, I., Luitjens, S., Ponti, M. and Boter, J. (2021) *Digitranscope: The Governance of Digitally-Transformed Society*, EUR 30590 EN; JRC 123362; Publications Office of the European Union, Luxembourg, <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digitranscope-governance-digitally-transformed-society>
- Datta, A. (2018) 'The digital turn in postcolonial urbanism: smart citizenship in the making of India's 100 smart cities', *Trans Inst Br Geogr.*, Vol. 43, pp.405–419, <https://doi.org/10.1111/tran.12225>
- Delacroix, S. and Lawrence, N. (2019) 'Bottom-up data trusts: disturbing the 'one size fits all' approach to data governance', *International Data Privacy Law*, Vol. 9, No. 4, <https://academic.oup.com/idpl/article/9/4/236/5579842/>, doi: <https://doi.org/10.1093/idpl/ipy014>
- DPDPB (2018) *The Draft of Personal Data Protection Bill 2018*, https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf (Accessed 7 September, 2022).
- DPDPB (2022) *The Digital Personal Data Protection Bill 2022*, https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Potection%20Bill%2C%202022_0.pdf
- Duan, Y., Edwards, J.S. and Dwivedi, Y.K. (2019) 'Artificial intelligence for decision making in the era of big data—evolution, challenges and research agenda', *International Journal of Information Management*, Vol. 48, pp.63–71, <https://doi.org/10.1016/j.ijinfomgt.2019.01.021>
- Durnell, E., Okabe-Miyamoto, K., Howell, R.T. and Zizi, M. (2020) 'Online privacy breaches, offline consequences: construction and validation of the concerns with the protection of informational privacy scale', *International Journal of Human–Computer Interaction*, Vol. 36, No. 19, pp.1834–1848, doi: 10.1080/10447318.2020.1794626.
- Dwivedi, Y.K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P.V., Janssen, M., Jones, P., Kar, A.K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., Medaglia, R., ..., Williams, M.D. (2021) 'Artificial intelligence (AI): multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy', *Int. J. Inf. Manag.* 2019, Vol. 57, p.101994, DOI: 10.1016/j.ijinfomgt.2019.08.002.
- Fadler, M. and Legner, C. (2022) 'Data ownership revisited: clarifying data accountabilities in times of big data and analytics', *Journal of Business Analytics*, Vol. 5, No. 1, pp.123–139, <https://doi.org/10.1080/2573234X.2021.1945961>
- Fia, T. (2021) 'An alternative to data ownership: managing access to non-personal data through the commons', *Global Jurist*, Vol. 21, No. 1, pp.181–210, <https://doi.org/10.1515/gj-2020-0034>
- Gangadharan, S.P. (2014) 'Data-based discrimination', in Gangadharan, S.P., Eubanks, V. and Barocas, S (Eds.): *Data and Discrimination: Collected Essays*, Open Technology Institute, https://timlibert.me/pdf/2014-data_Discrimination_Collected_Essays.pdf

- Gekker, A. and Hind, S. (2019) 'Infrastructural surveillance', *New Media Society*, Vol. 22, pp.1414–1436.
- Gellert, R. (2020) 'Comparing definitions of data and information in data protection law and machine learning: a useful way forward to meaningfully regulate algorithms?', *Regulation and Governance*, p.16, DOI: 10.1111/rego.12349.
- Ghosh, D. (2021) 'The commercialization of bias in cashless India', *Telecommunications Policy*, Vol. 45, No. 5, p.102124, ISSN 0308-5961, <https://doi.org/10.1016/j.telpol.2021.102124>
- Giannopoulou, A., Ausloos, J., Delacroix, S. and Janssen, H. (2022) 'Intermediating data rights exercises: the role of legal mandates', *International Data Privacy Law*, Vol. 12, No. 4, pp.316–331, <https://doi.org/10.1093/idpl/ipac017>
- Hardinges, J. (2018) *What is a Data Trust?*. Open Data Institute, <https://theodi.org/article/what-is-a-data-trust/>
- Hardinges, J. and Wells, P. (2018) *Defining a 'Data trust'*, Open Data Institute from <https://theodi.org/article/defining-a-data-trust>
- Harris, T. and Wyndham, J. (2015) 'Data rights and responsibilities: a human rights perspective on data sharing', *Journal of Empirical Research on Human Research Ethics*, Vol. 10, pp.334–337, DOI: 10.1177/1556264615591558.
- Haupt, M. (2016) *Data is the New Oil – A Ludacris Proposition*, Project 2030 Blog, 6 May, 2016, <https://medium.com/project-2030/data-is-the-new-oil-a-ludicrous-proposition-1d91bba4f294> (Accessed 27 February, 2019).
- Hazel, S. (2020) *Personal Data as Property*. *Syracuse Law Review*, SSRN: <https://ssrn.com/abstract=3669268> or <http://dx.doi.org/10.2139/ssrn.3669268>
- Hicks, J. (2023) 'The future of data ownership: an uncommon research agenda', *The Sociological Review*, Vol. 71, No. 3, pp.544–560, <https://doi.org/10.1177/00380261221088120>
- Hobbes, T. (1651) *Leviathan*, Project Gutenberg (Original work published 1651).
- Hummel, P., Braun, M. and Dabrock, P. (2021) 'Own data? ethical reflections on data ownership', *Philos. Technol.*, Vol. 34, pp.545–572, <https://doi.org/10.1007/s13347-020-00404-9>
- IDABNUP (2022) *India Data Accessibility Background Note and Use Policy*, February, <https://www.meity.gov.in/writereaddata/files/Background%20Note%20for%20India%20Data%20Accessibility%20and%20Use%20Policy.pdf>
- IDAUP (2022) *India Data Accessibility and Use Policy*, February, https://www.meity.gov.in/writereaddata/files/Draft%20India%20Data%20Accessibility%20and%20Use%20Policy_0.pdf
- Ithurbide, C., Bouquillion, P., Parthasarathi, V. and Sneha, P.P. (2023) 'Introduction: platform challenges to creative industries in India', *Contemporary South Asia*, Vol. 31, No. 2, pp.268–275, doi: 10.1080/09584935.2023.2203904.
- ITR (2011) *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data Or Information) Rules*.
- JBNSCR (2018) *Justice, B.N. Srikrishna Committee Report*, Data Protection Framework, https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
- Jones, C.I. and Tonetti, C. (2020) 'Nonrivalry and the economics of data', *American Economic Review*, Vol. 110, No. 9, pp.2819–2858 <https://doi.org/10.1257/aer.20191330>
- JPCR (2021) *Joint Parliamentary Committee Report ('JPC Report') on the Personal Data Protection Bill, 2019 ('PDPB')*, https://drive.google.com/file/d/1emcAB8HjE2oCC_DI6zR5YPnPQ5iwwwCT/view.
- Kamarinou, D., Millard, C. and Singh, J. (2016) *Machine Learning with Personal Data* (November 7, 2016), Queen Mary School of Law Legal Studies Research Paper No. 247/2016, Available at SSRN: <https://ssrn.com/abstract=2865811>
- Kitchin, R. (2014) *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*, Sage, Thousands, Oaks, CA.

- Lightfoot, G. and Wisniewski, T.P. (2014) 'Information asymmetry and power in a surveillance society', *Inf. Organ.*, Vol. 24, pp.214–235.
- Locke, J. (1689) *Two Treatises of Government*. Project Gutenberg (Original work published 1689).
- Lugano, G. (2017) 'Virtual assistants and self-driving cars', *2017 15th International Conference on ITS Telecommunications (ITST)*, Warsaw, Poland, pp.1–5.
- Lund, J. (2011) Property rights to personal information', *Northwestern J. Technology and Intellectual Property*, Vol. 10, No. 1, pp.1–18.
- Malik, P.K., Singh, R., Gehlot, A., Akram, S.V. and Das, P.K. (2022) *Village 4.0: Digitalization of Village with Smart Internet of Things Technologies, Computers and Industrial Engineering*, Vol. 165, <https://doi.org/10.1016/j.cie.2022.107938>
- Manyika, J., Chui, M., Miremadi, M., Bughin, J., George, K., Willmott, P. and Dewhurst, M. (2017) *A Future That Works: Automation, Employment, and Productivity*, McKinsey Global Institute.
- McBride, K. (2018) *Monetizing Smart Cities: Framing the Debate*, CIGI, Data Governance in the Digital Age Special Report, www.cigionline.org/articles/monetizing-smartcitydata?utm_source=twitter&utm_medium=social&utm_campaign=data-series
- McDonald, S. (2019) *The Fiduciary Supply Chain*, Centre for International Governance Innovation, <https://www.cigionline.org/articles/fiduciary-supply-chain>
- MeitY (2019) *Report by the Committee of Experts on Non-Personal Data Governance Framework*, Ministry of Electronics and Information Technology, accessible at <https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf>
- Mir, U.B., Kar, A.K. and Gupta, M.P. (2020a) 'Digital identity evaluation framework for social welfare', in Sharma, S.K., Dwivedi, Y.K., Metri, B. and Rana, N.P. (Eds.): *Re-Imagining Diffusion and Adoption of Information Technology and Systems: A Continuing Conversation. TDIT 2020, IFIP Advances in Information and Communication Technology*, Vol. 617, Springer, Cham, https://doi.org/10.1007/978-3-030-64849-7_36
- Mir, U.B., Kar, A.K., Dwivedi, Y.K., Gupta, M.P. and Sharma, R.S. (2020b) 'Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India', *Government Information Quarterly*, Vol. 37, No. 2, pp.1–52, https://cronfa.swan.ac.uk/Record/cronfa53060/Download/53060_16145_30bafc2d109c485089258f5cac663025.pdf
- Nagaraj, A., Singh, S. and Yasa, V.R. (2021) Factors affecting consumers' willingness to subscribe to over-the-top (OTT)', *Video Streaming Services in India, Technology in Society*, Vol. 65, p.101534, ISSN 0160-791X, <https://doi.org/10.1016/j.techsoc.2021.101534>
- Nsai (2018) NITI Ayog. June (2018) Discussion Paper National Strategy for Artificial Intelligence, <https://indiaai.gov.in/documents/pdf/NationalStrategy-for-AI-Discussion-Paper.pdf>
- Paine, T. (2012) *Rights of Man*. Digireads.com Publishing (Original work published 1791).
- Paprica, P.A., Sutherland E., Smith, A., Brudno, M., Cartagena, R.G., Crichlow, M., Courtney, B.K., Loken, C., McGrail, K.M., Ryan, A., Schull, M.J., Thorogood, A., Virtanen, C. and Yang, K. (2020) 'Essential requirements for establishing and operating data trusts: practical guidance co-developed by representatives from fifteen Canadian organizations and initiatives', *International Journal of Population Data Science*, Vol. 5, No. 1, p.1353, <https://doi.org/10.23889/ijpds.v5i1.1353>
- Paunksnis, S. (2023) 'India digitalized: surveillance, platformization, and digital labour in India', *Inter-Asia Cultural Studies*, Vol. 24, No. 2, pp.297–310, DOI: 10.1080/14649373.2023.2182942.
- PDPB (2019) *The Personal Data Protection Bill 2019*, https://prsindia.org/files/bills_acts/bills_parliament/2019/Personal%20Data%20Protection%20Bill,%202019.pdf (Accessed 16 November, 2022).
- Pinsent Masons and Ors. (2019) *Data Trusts: Legal and Governance Considerations*, <https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf>

- Pozen, D.E. and Khan, L.M. (2019) 'A skeptical view of information fiduciaries', *Harvard Law Review*, <https://harvardlawreview.org/2019/12/a-skeptical-view-of-information-fiduciaries/>
- PRAI (2021) *NITI Aayog . February 2021. RESPONSIBLE AI #AIFORALL: Approach Document for India Part 1 – Principles for Responsible AI*, <https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf>
- Prasad, S.M. (2019) *Information Fiduciaries and India: s Data Protection Law*, Data Analyst.
- Prince, C. (2017) 'Do consumers want to control their personal data? Empirical evidence', *International Journal of Human-Computer Studies*, p.110, DOI: 10.1016/j.ijhcs.2017.10.003.
- Purtova, N. (2018) 'The law of everything. broad concept of personal data and future of EU data protection law', *Law, Innovation and Technology*, Vol. 10, No. 1, pp.40–81, DOI: 10.1080/17579961.2018.1452176.
- Quach, S., Thaichon, P., Martin, K.D., Weaven, S. and Palmatier, R.W (2022) 'Digital technologies: tensions in privacy and data', *J. of the Acad. Mark. Sci.*, Vol. 50, pp.1299–1323, <https://doi.org/10.1007/s11747-022-00845-y>
- Raina, A. and Palaniswami, M. (2021) *The Ownership Challenge in the Internet of Things World*, Technology in Society, Vol. 65, <https://doi.org/10.1016/j.techsoc.2021.101597>
- RAITF (2018) *The Report on the Artificial Intelligence Task Force*, p.1, http://dipp.nic.in/sites/default/files/Report_of_Task_Force_on_ArtificialIntelligence_20March2018_2.pdf
- Rajam, V., Reddy, A.B. and Banerjee, S. (2021) *Explaining Caste-Based Digital Divide in India*, *Telematics and Informatics*, Vol. 65, p.101719, <https://doi.org/10.1016/j.tele.2021.101719>
- Risse, M. (2021) *Data as Collectively Generated Patterns: Making Sense of Data Ownership*, Carr Center for Human Rights Policy, https://carrcenter.hks.harvard.edu/files/cchr/files/210426-data_ownership.pdf
- Rousseau, J.J. (1762) *The Social Contract*. Project Gutenberg (Original work published 1762).
- Sam, J.S., Ray, R. and Chakraborty, A. (2023) 'Digital payments on the agenda: how supply-side actors framed cash and digital payments during the COVID-19 pandemic in India', *Asian Studies Review*, Vol. 47, No. 2, pp.336–354, DOI: 10.1080/10357823.2022.2063253.
- Saracini, N. and Shanmugavelan, M. (2019) *BOND: Caste and Development*.
- Schäfer, M.T. and van Es, K. (2017) *The Datafied Society Studying Culture Through Data*, Amsterdam University Press, Amsterdam.
- Schwartz, P.M. (2004) 'Property, privacy, and personal data', *Harvard Law Review*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=721642
- Schwartz, R., Dodge, J., Smith, N.A. and Etzioni, O. (2020) *Green, A.I. Communications of the ACM*, Vol. 63, No. 12, pp.54–63, <http://dx.doi.org/10.1145/3381831>
- Singh, S.S. (2011) 'Privacy and data protection in India: a critical assessment', *Journal of the Indian Law Institute*, Vol. 53, No. 4, pp.663–677, <http://www.jstor.org/stable/45148583>
- Sivarajah, U., Kamal, M.M., Irani, Z. and Weerakkody, V. (2017) 'Critical analysis of big data challenges and analytical methods', *Journal of Business Research*, Vol. 70, pp.263–286, <https://doi.org/10.1016/j.jbusres.2016.08.001>
- Stepanov, I. (2020) 'Introducing a property right over data in the EU: the data producer's right – an evaluation', *International Review of Law, Computers and Technology*, Vol. 34, No. 1, pp.65–86, DOI: 10.1080/13600869.2019.1631621.
- Supreme Court of India (2017) *Justice KS Puttaswamy and Ors vs Union of India and Ors (2017) 10 SCC 1*.
- Tewathia, N., Kamath, A. and Ilavarasan, P.V. (2020) *Social Inequalities*, fundamental inequities, and recurring of the digital divide: Insights from India, *Technology in Society*, Vol. 61, p.101251, ISSN 0160-791X, <https://doi.org/10.1016/j.techsoc.2020.101251>
- Torra, V. (2023) 'Data privacy for machine learning and statistics', *Handbook of Statistics*, Elsevier, <https://doi.org/10.1016/bs.host.2023.06.003>
- Valerian Rodrigues (2011) 'Justice as the lens: interrogating rawls through Sen and Ambedkar', *Indian Journal of Human Development*, Vol. 5, No. 1, pp.153–174.

- Venkataramanan, R., Kumar, A., Mantena, S. and Subramanian, S.V. (2021) 'Geographical variation in mobile phone ownership and SMS literacy among women (age in India: a cross-sectional analysis based on national family health survey-4)', *Technology in Society*, Vol. 64, p.101482, ISSN 0160-791X, <https://doi.org/10.1016/j.techsoc.2020.101482>, 5-49
- Verma, A. and Gurtoo, A. (2021) *Evaluating Global Data Policies around Non-Personal Data. IISc-CSP*, Centre for Society and policy. India, Retrieved from <https://policycommons.net/artifacts/3346922/verma-a/4145822/> on 15 August, 2023, CID: 20.500.12592/hfz4rn
- Vial, G. (2023) 'Data governance and digital innovation: a translational account of practitioner issues for IS research', *Information and Organization*, Vol. 33, No. 1, <https://doi.org/10.1016/j.infoandorg.2023.100450>
- Victor, J. (2013) 'The EU general data protection regulation: toward a property regime for protecting data privacy', *Yale Law Journal*, <https://www.yalelawjournal.org/comment/the-eu-general-data-protection-regulation-toward-a-property-regime-for-protecting-data-privacy/>
- Virginia Eubanks (2014) 'Big data and human rights', in Gangadharan, S.P., Eubanks, V. and Barocas, S. (Eds.): *Data and Discrimination: Collected Essays*, Open Technology Institute, New America, https://timlibert.me/pdf/2014-Data_Discrimination_Collected_Essays.pdf (Accessed 5 November, 2014).
- Westendorf, L., Shaer, O., Pollalis, C., Verish, C., Nov, O. and Ball, M.P. (2018) 'Exploring genetic data across individuals: design and evaluation of a novel comparative report tool', *J. Med Internet Res.* 24, Vol. 20, No. 9, p.e10297, DOI: 10.2196/10297.
- Whitt, R.S. (2020) 'Old school goes online: exploring fiduciary obligations of loyalty and care in the digital platforms era', *Santa Clara High Technology Law Journal*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3427479
- Williams, J. (2018) *Stand Out of our Light: Freedom and Resistance in the Attention Economy*, Cambridge University Press, Cambridge.
- Wilson, H.J. and Daugherty, P.R. (2018) *Human + Machine: Reimagining Work in the Age of AI*, Harvard Business Review Press, Boston, MA.
- Yu, X. and Zhao, Y. (2019) 'Dualism in data protection: balancing the right to personal data and the data property right', *Computer Law and Security Review*, Vol. 35, No. 5, <https://doi.org/10.1016/j.clsr.2019.04.001>
- Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, New York.