SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 2 | February 2026 - Peer Reviewed Journal

THE RIGHT TO PRIVACY AND THE DIGITAL ECONOMY: AN EXAMINATION OF THE IMPACT OF INDIA'S DATA PROTECTION REGIME ON E-COMMERCE AND FINTECH

Samraat Singh[1], Dr. Ajeet Kumar[2]
[1]*Research Scholar, Department of Law, Major S. D. Singh University, Farrukhabad (U.P.)*
[2]*Associate Professor, Department of Law, Major S. D. Singh University, Farrukhabad (U.P.)*

Article DOI: https://doi.org/10.36713/epra25992
DOI No: 10.36713/epra25992

ABSTRACT

India's development as one of the world's fastest-growing digital economies has fuelled a higher level of scholarly debate about the intersection between the right to privacy and data-driven commerce. The rise of e-commerce and financial technology (fintech) services has meant that personal information has become a valuable economic asset, thereby waking up concerns about strong protection of that data.

In this manuscript, I critically consider the implications of India's data protection regime (in the form of the Digital Personal Data Protection Act, 2023 (DPDP Act)) on privacy rights in the e-commerce and fintech domain. Relying on constitutional jurisprudence, legislation, and case law, I examine the duality of how privacy is both protected and diluted in a digital marketplace that is engulfed by profiling, a lack of assenting parties, and surveillance.

The analysis places India's framework vis-a-vis other global leaders, reflecting on policy against global practices like GDPR, providing analytical insights into enforcement challenges. -Who must comply, under what enforcement mechanisms, and civil penalties? The framework for cross-border data in the event of violation(s) of this framework, enforcement mechanisms, fines/penalties for non/pro негo compliance. been activated, the debt recovery process will subscribe. Private contracts carry out involved parties are enabled to subscribe to the actions.

It urges that, in addition to bolstering trust between the consumer and the private producer, the DPDP Act's exemption of certain scenarios and enforcement limitations create potential risks to achieving a privacy-centric economy.

KEYWORDS: *Right to Privacy, Digital Personal Data Protection Act 2023, Informational Privacy, E-commerce, Fintech, Consumer profiling, Data Localization.*

1. INTRODUCTION

India's digital economy has been transformed in a profound way, with a slew of e-commeric platforms such as Amazon, Flipkart and fintech applications such as Paytm, PhonePe and Google Pay redefining the consumer lifestyles. The fast and rapid growth of these sectors is powered by data collection capabilities and predictive analytics capabilities, which in turn enables personalization, targeted advertising and financial inclusion. However, this data dependence brings particularly serious questions about privacy violating, categorization and profiling without authorization, and the commodification of the personal data. The acceptability of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017) extended the purview of the right to privacy to include informational privacy and consequently placed new obligations on both the state and private actors. The enactment of the DPDP Act, 2023 that followed is a significant legislative challenge in trying to regulate the usage of a data, particularly for commercial purposes. This paper is a critical study of the effect of such a legal framework on privacy rights in the digital economy whereby e-Commerce and fintech take a special focus as they are the central participants where data protection affects consumer trust, compliance by organisations with relevant laws and market stability.

2. REVIEW OF LITERATURE

As the evolving constitutional scholarly commentary on the relationship between privacy and commerce in India points to this articulation of this triad, comprising constitutional norms, technological change, and market governance. Scholars are always maintaining that privacy is not only an issue of civil liberty and a central element in the sustainability of economic markets in the digital environment. Baxi (2018) explains in this context why, after Puttaswamy, privacy lurks in the larger economic rights policy where safeguarding personal data as the role of technology companies is to foster consumer confidence in using digital platforms: Abraham and Hickok (2019) highlight how India's draft data protection framework comes into pendulum swings between innovating through data and protecting the individual's rights leading to compromising enforcement and regulatory criminality. Chander and Le (2020) place India's proposals against theirs in a GDPR comparison, highlighting the lack of robust consent structures and the enforcement capacity which makes India's protections relatively fragile.

The literature on fintech adoption flags up rapid consumer experience as a result of accessibility and efficiency but highlights in the absence of harsh accountability frameworks the systemic vulnerabilities. "I think this concern is enhanced by research from around

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 2 | February 2026 - Peer Reviewed Journal

the world." Schwartz and Peifer (2017) show that robust and enforceable data protection laws, like GDPR, both drink the nectar of innovation, as they give legal clarification to businesses. Empirical analyses also advanced the view that trust in digital systems directly correlates with the robustness of data protection legislation, and thus, for sustainable digital commerce, the strength of the regulation is a prerequisite.

Judicial contributions are also an important part of the literature. For example, the question in Internet and Mobile Association of India v. RBI (2020) The dilemma of co-existing regulatory supervision and economic innovation is demonstrated by the way in which the courts moderate the confrontation between regulatory oversight and economic innovation. Earlier rulings like PUCL v. Union of India (1997) and the very recent case of Rajiv Mohan Tom v Union of India. While these cases provide a way to read the Act of Parliament on certain aspects, academic work suggests a continuing research deficit in the issues of direct implications of India's DPDP Act, 2023 on the e-community and fintech sector. This lacuna underscores the gap for a doctrinal and analytical study-primarily in the context of the Indian experience-in a constitutional theory as well as comparative international to give a foundation to evaluate privacy as a structural part of digital economy.

3. METHODOLOGY

This paper involves a doctrinal and analytical research method, which relies on primary sources such as provisions of the constitution, legislations and court judgments. The DPDP Act, 2023, and the guidelines of RBI are the statutory ground of analysis. Secondary sources include peer reviewed journals, commentaries and reports by regulatory bodies. A comparative framework in light of GDPR and U.S. data laws for providing a global background to the process is offered, which provides for a normative analysis of the distinctive policy choices made in India.

4. PRIVACY AS A CONSTITUTIONAL RIGHT: AN EXAMINATION OF CONSTITUTIONAL PRINCIPLES

The Fundamental right of Privacy has been established by Justice K.S. Puttaswamy v. Union of India [R (2)]. Union of India (2017) comes out as a watershed moment in the development of data protection discourse in India. Under the unanimous judgment of the bench, informational privacy being an integral function of the right to life and personal liberty, used to endow informational privacy with the status of a constitutional right. In the course, the Court derived three different dimensions of privacy - the bodily, the spatial, and the informational - with the latter being particularly relevant for the regulation of digital commerce. Informational privacy here refers to someone's right to decide how their personal information is gathered, stored, processed, and distributed - which has immediate implications for e-commerce and fintech platforms whose functions depend on the massive mobilisation and utilisation of data.

The biggest doctrinal contribution arising out of the Puttaswamy judgment was the insertion of a proportionality test. Securing Privacy: This test brings to bear a triptych of a duty for states to comply with, whenever the state might cause interference with solitude: legality (statutes would be needed); necessity (a legitimate goal would be served); and proportionality (the least restrictive alternative or means would be needed). The framework not only regulates state surveillance but it also sets a constitutional standard against which private sector processing of data should be compared. In the face of an economy defined by algorithmic profiling, predictive analytics and behavioural targeting, proportionality is a bulwark against excessive and exploitative data practices.

This constitutional preference was further embedded in previous provisions. In PUCL v. Union of India (1997), the Supreme Court emphasized the need for procedural safeguards intended to prevent arbitrary telephone tapping - a principle that echoes in the current arguments regarding electronic surveillance and monitoring of online activities. Equality also applies in District Registrar and Collector v. Thus, Canara Bank (2005), held that the right to privacy is applicable to, among other things, banking and information, thus foreshadowing the issues that are currently being raised in relation to maintaining the confidentiality of financial data. Taken as a whole, these cases confirm that privacy is no longer restricted to the private sphere but is also connected to commercial and economic contexts where personal data rightfully flows.

Moreover, the constitutional protection available to privacy is in harmony with the Directive Principles of State Policy especially Article 38 which directs the state to ensure social and economic justice. The protection of informational privacy within the digital economy is therefore able to be framed as an economic justice move, shielding citizens against relationships of unequal power that exist between corporations and consumers. This trend is also confirmed by comparative jurisprudence: the European Court of Human Rights, for example, has taken over data protection as part of Article 8 of the European Convention on Human Rights (which explicitly provides for the protection of personal data), thereby emphasizing that data protection is part of the human dignity and the democratic accountability.

Hence the constitutional framework is the normative pillar for the digital governance in India. Finally, it puts into perspective the commercial innovation in growth areas for the economy, such as e-commerce and fintech, in harmony with the founding values of the financial transformation of the constitution, which are dignity, autonomy, and freedom. By acknowledging informational privacy as a part of the fundamental rights itself, the judiciary gives a responsibility to both the state and private individual for following

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 2 | February 2026 - Peer Reviewed Journal

constitutional morality in their data-holding practices. This solution is not just justified by the principle that assimilates the working of the economy, but it also ensures that the policy of economic efficiency does not overshadow the demand of constitutional justice underlying the magnitude of the interventions under the Digital Personal Data Protection Act, 2023.

5. STATUTORY FRAMEWORK DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is the first extensive effort made by the Government to protect personal data through the law in the increasingly prominent digital economy. Its statutory design portrays a considered balance between development of innovation and constitutional privacy. A careful reading of the Act, especially in regards to e-commerce and fintech, shows impressive strengths and exposed weaknesses.

i. Consent Architecture (Sub-section 6):

The Act enshrines consent as being the lawful basis for processing. Consent needs to be free, knowledgeable, specific and clear. However, the definition only admits to an "exception on deemed consent," which actually weakens this threshold allowing for data processing to take place without explicit consent in so-called "state functions" and for the processing of data that would reasonably be placed at the disposal of a user of the personal data. In particular, for e-commerce, the provision runs the risk of policing consent - meaning legitimizing intrusive profiling - by burying it in the terms-of-service contract**.**

ii. Provision of Purpose and Data Minimization (Section 7 and 8)

These requirements include collecting data for a certain lawful purpose and not processing the data unnecessarily. If hard put into practice, this principle would prevent the ubiquitous cross-platform profiling of e-commerce behemoths. However, the expansive interpretations to which the hazy definition of "necessary for service" is open to render down privacy protections.

iii. Rights of Data Principals: (Figures 12-15)

The Act gives rights such as access, correction, erasure and grievance redressal rights. On the side of fintech users, this statutory recognition has enormous implications, bringing constitutional privacy of individuals to routine everyday commercial activities. However, scholars have written about the fact that without proper enforcement mechanisms, these rights can remain as "paper rights" (Abraham & Hickok, 2019).

iv. Exemptions granted by the government (Section 17)

A major weakness is the fairly large loophole to allow government agencies, on the basis of national security and public order, among other things. Such carve out by the legislature gives the specter of 'surveillance creep', especially when personal financial and consumer data is collaged into state-led digital ecosystems such as Aadhaar or UPI.

v. Institutional Review - Data Protection Board (Section 19)

The Act forms a regulatory body, the Data Protection Board. Like the criticisms of Indian regulatory institutions in the past, its independence and capability have also been questioned. In contrast to the empowered supervisory authorities in the GDPR, the Board seems to be more administrative than quasi-judicial in nature and, therefore, to have less capacity to hold powerful private actors to account for their actions.

vi. Sectoral Implications

- For example, in e-commerce, despite the now-widespread expectation of notice and optin mechanisms, the process remains difficult to enforce because of consumer digital illiteracy.
- Regulatory: Companies are required to deploy strong controls for financial information as per RBI guidelines, but the entities are facing regulatory overlaps, resulting in uncertain compliance and compliance fatigue.

6. E-COMMERCE, PROFILE OF CONSUMERS, DATA GOVERNANCE

E-commerce is the key building block of the Indian digital economy, which marries a heavy dependency on consumer data to inform personalisation and targeted advertising. The Personal Data Protection Bill (DPDP) aims to regulate this area but is faced with massive structural challenges.

i. Algorithmic Profiling and Behavioural Targeting

Departments of the likes of Amazon and Flipkart use sophisticated and sound predictive algorithms to segment users, thereby manipulating buying decision through recommendation engines. Though such practices offer great economic efficiency, at the same time they infringe much informational privacy, this way blurring the difference between personalization and manipulation.

ii. Data Breach and Systemic Risks

India has seen its share of data breaches with some of the greatest examples such as Juspay in 2020, and the breach of BigBasket in 2021 which affected millions of personal records. These episodes reveal some underlying systemic vulnerabilities that are corroding consumer trust while legal remedies are still not well developed. Despite the mandates of Section 8 to minimize data, the low levels of enforcement around cybersecurity provisions mean that such data protection is undermined.

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 2 | February 2026 - Peer Reviewed Journal

iii. **Consent Imbalance and Asymmetrical Information**
While the Act purports that informed consent must be sought, the empirical research suggests that consumers rarely read or understand privacy policies because of the inherent complexity of such policies. This circumstance breeds a "consent asymmetry," in which businesses take advantage of the term gap between nominal consent and real comprehension (Schwartz & Peifer, 2017).

iv. **Data Minimization (Section 8)**
Section 8 states that only necessary information is permissible to collect theoretically limiting profiling practices. However, the lack of exact criteria on what defines "necessary" allows the platforms to justify aggregation of too much data under the umbrella of operational efficiency.

v. **Grievance Redressal Mechanism**
The DPDP Act proves to establish a right to grievance redressal; however, this coupled with the absence of any sector-specific mechanism of dispute resolution means that consumers have to depend on company-operated channels. Given the asymmetry of power, such frameworks can hardly offer meaningful empowerment to consumers.

vi. **Comparative Insights**
The General Data Protection Regulation provides for strict safeguards for profiling used in automated decision-making and individual rights of human intervention, including widespread centralised review. India does not have the same protections in its law and so consumers are left vulnerable to some shady dealings by algorithms.

vii. **Impact on Consumer Trust**
Empirical studies prove time and again that trust is a conditioning foundation for digital adoption. Weak enforcement of statutory safeguards threatens this trust, which can discourage long term growth of e-comm. Accordingly, even though the DPDP Act is a progressive effort, it fails to include strict checks necessary to maintain privacy in the face of commercial exigencies.

7. FINTECH AND FINANCIAL PRIVACY: THE REGULATORY CROSSROADS

The fintech sector in India occupies a particularly sensitive position within the broader digital economy, since it processes not only identifiers but also transactional histories, credit scores, and behavioral financial footprints. The risks associated with misuse of such data extend beyond reputational harm to tangible economic consequences, including fraudulent transactions, identity theft, and systemic exclusion from credit markets. Against this backdrop, both statutory and regulatory frameworks have attempted to establish safeguards, but the resulting overlap has often generated confusion.

The Reserve Bank of India (RBI) has been proactive in setting standards on cybersecurity and data localization, particularly through its 2018 and 2021 circulars that require payment system providers to store all transaction data within India. These measures align with the DPDP Act's emphasis on purpose limitation and accountability but also impose high compliance costs on global fintech entities operating in India. The rationale of sovereignty and consumer protection is clear, yet the strict localization mandates complicate the free flow of capital and data across jurisdictions.

Judicial interventions have further highlighted the delicate balance between innovation and regulation. In Internet and Mobile Association of India v. RBI (2020), the Supreme Court invalidated the RBI's blanket prohibition on virtual currency transactions, reasoning that disproportionate restrictions undermine innovation while failing to adequately serve legitimate policy objectives. The Court's reliance on proportionality analysis signals that regulatory frameworks governing fintech must remain both constitutionally valid and technologically adaptive.

The DPDP Act's contribution to fintech privacy primarily lies in its recognition of rights of data principals under Section 15, including rights to correction and erasure. These provisions allow users to demand deletion of redundant KYC data or correction of financial records, thereby enhancing individual control over sensitive information. Yet, the practical enforcement of these rights remains doubtful given the absence of sector-specific adjudicatory mechanisms and the reliance on a Data Protection Board whose independence is contested.

The regulatory overlaps are particularly pronounced in digital lending, where platforms often rely on invasive access to mobile metadata to assess creditworthiness. While the RBI's 2022 digital lending guidelines prohibit such practices without explicit consent, the DPDP Act does not address algorithmic credit scoring with equivalent precision. The result is a fragmented regime where fintech firms must reconcile DPDP obligations with RBI compliance requirements, often at the cost of clarity and innovation. Unless harmonization between sectoral regulators and the DPDP framework is achieved, India risks cultivating a fintech ecosystem where consumer privacy is nominally recognized but practically undermined.

8. COMPARATIVE PERSPECTIVES: BOTH GDPR AND MORE

A comparison of India's statutory framework with the international regimes on data protection has been done to shed light on the promise and limits of the law in India. The General Data Protection Regulation (GDPR) in the European Union stays the gold standard for strong implementation, with data protection supervisory authorities which are institutionally independent, have the

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 2 | February 2026 - Peer Reviewed Journal

power to impose up to four per cent of global turnover fines, and have jurisdiction over extra-national movements of data. Importantly, Article 22 of the GDPR also entails contactable provisions on safeguarding profiling and automated decision-making, which ensure that consumers currently continue to benefit from the right to human scrutiny over algorithmic credit or services decisions. The absence of such safeguards in India's Data Protection Bill (DPDP Act) leaves a regulatory gap when it comes to protection of Fin/thems, which disproportionately leaves the Fin consumers at the receiving end of opiate data credit scoring and behavioural profiling.

The United States represents an alternative model, which is regionalized. There are existing laws like Gramm-Leach-Bliley, HIPAA, and COPPA, which govern financial information, health information, and children's privacy respectively. While this structure has provided flexibility and the ability to define the regulatory areas for each sector separately it has also created gaps in the regulations especially in emerging areas of fintech such as cryptocurrency exchanges and digital wallets. India's DPDP Act is making an attempt to create a unified framework but suffers similar gaps as the BTCA on enforcement, although it tries to overcome fragmentation by sub-sectors, and overlaps with sectoral regulators (such as the RBI, SEBI), thus replicating the coordination deficiencies in the U.S.

Beyond the transatlantic models, there are instructive regional comparisons on offer in Asian jurisdictions. Singapore's Personal Data Protection Act (PDPA) operates from the angle of minimizing corporate flexibility while ensuring enforceable requirements of consent; while China's Personal Information Protection Law (PIPL) is strict in the geological context by the requirement of data localization and the involvement of national state sovereignty. India's approach seems to be a hybrid of both, where the emphasis is on compliance facilitation, and on the other hand data sovereignty. However, as opposed to the clarity of Singapore or the vigor of China, India's framework suffers from definitional vagueness and institutional independence, which calls into question the ability of the framework to provide substantive privacy protection in practice.

In this comparative landscape, the challenge for India will therefore be to formulate a data protection regime that is not only proportional and dignified in accordance with the Constitution, but also conducive to consumer trust and global competitiveness. While the GDPR is proof that strict enforcement is not incompatible with innovation, India's reliance on exemptions and facilitative compliance runs the risk of building a system of formalized law which either leaves little room for a commitment to privacy or drags it out**.**

9. CONCLUSIONS AND POLICY RECOMMENDATIONS

It is clear from the development of electronic commerce and financial technologies in India and the trajectory of digital economy, that privacy is not peripheral issue, but a developmental structural prerequisite for making an e-commerce and Fintech sector sustainable. The establishment of privacy as a fundamental right in Puttaswamy has elevated the concept of informational autonomy from merely being an aspirational constitutional right to a constitutional mandate; and the Digital Personal Data Protection Act, 2023 fully operationalizes this mandate for the first time. Yet, the Act has some large gaps. While it introduces fundamental principles such as consent, data minimisation and user rights, its exemptions for the public sector, lack of institutional independence and mechanisms of penalty are rather limited in several respects, making both accountability and trust likely to be diluted.

Consumer tracking is essentially the engine of the business model in e-commerce, so if this business model is to make the jump from personalization to surveillance, there needs to be improved enforcement. In fintech, where financial privacy is the cornerstone for inclusion and innovation, non-integrated regulatory requirement between the DPDP Act and RBI guidelines, palpably generates uncertainty that is a strong disincentive to responsible innovation. Unless there is harmonisation, privacy protection will remain symbolic not substantive.

The autonomy and capability of the Data Protection Board, harmonizing statutory requirements with constitution of sectoral regulators like RBI, and addition of stronger deterrence to pressurize operational faults should thus be the key areas of focus in policy reform. Also key is the advancement of digital literacy so that consumers will be able to effectively exercise their rights. Lessons from the GDPR make it clear that when fairly transacted, privacy protections not only conclude in the protection of dignity but also ensure that they may result in an increase of innovation as well as global competitiveness.

A digital economy which protects privacy is thus not just a legal imperative, it is an economic imperative - one that guarantees a normatively consistent meaning of growth in e-commerce and fintech for India in keeping with constitutional and international best practices.

REFERENCES

1. *Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.*
2. *Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274.*
3. *People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.*
4. *Digital Personal Data Protection Act, 2023 (India).*
5. *Reserve Bank of India, "Circular on Storage of Payment System Data" (2018).*

SJIF Impact Factor (2026): 8.863| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 11 | Issue: 2 | February 2026 - Peer Reviewed Journal

6. *Abraham, R. and Hickok, E., "Data Protection in India: The Draft Personal Data Protection Bill, 2018" (2019) Indian Journal of Law and Technology.*
7. *Baxi, U., The Future of Human Rights (OUP 2018).*
8. *Chander, A. and Le, U., "Data Nationalism" (2020) 64 Emory Law Journal 677.*
9. *Pal, R., "Financial Privacy and Digital Lending in India" (2021) Economic and Political Weekly, Vol. 56(12).*
10. *Schwartz, P. and Peifer, K., "Transatlantic Data Privacy Law" (2017) 106 Georgetown Law Journal 115.*
11. *Regulation (EU) 2016/679 (General Data Protection Regulation, GDPR).*
12. *Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999).*