INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CONSUMER INTEREST AND DATA PRIVACY IN E-COMMERCE: A CRITICAL ANALYSIS OF THE LEGAL FRAMEWORK IN INDIA

AUTHORED BY - ANJANA JANARDHANAN
LLM
Christ University, Pune Lavasa Campus

Abstract

The e-commerce industry in India has become one of the fastest-growing digital markets in the world, thanks to rising smartphone penetration and the low cost of internet access and the development of digital payment systems. Nevertheless, this fast development has been coupled with an unprecedented surge in the amassing, handling, and commercialization of consumer data. To make personalized services, targeted advertising, and operational efficiency possible, e-commerce platforms constantly accumulate large volumes of personal data, such as behaviour and transactional data, to collect large volumes of personal information. Although this type of practice improves the user experience, it also generates major concerns about informational privacy, data security, and consumer control. The establishment of privacy as a constitutional right in Justice K.S. Puttaswamy (Retd.) v. Union of India was the first constitutional breakthrough on the issue and the foundation of the Indian data protection system. The paper provides a critical analysis of how this developing legal framework is sufficient to address the issue of data privacy in the e-commerce ecosystem. The paper outlines the most important lapses in regulation, especially concerning transfers of data across borders, algorithmic profiling and the practical application of the principles of data minimization. The article maintains that these loopholes are causing less consumer confidence and heightened susceptibility to online payments. Through a doctrinal and comparative method, the paper notes the importance of having clearer regulatory standards, stronger enforcement mechanisms and more institutional coordination. It ends by suggesting specific legal and policy changes that should be implemented to strike the balance between innovation and strong consumer data protection in the Indian digital economy.

ISSN: 2582-6433

1. Introduction

Background and Significance

E-commerce business is one of the rapidly expanding digital economies in the world. The market will expand to approximately USD 280 to 300 billion in the year 2030 than in 2025 given the massive use of smartphones, low cost data and the rapid expansion of direct to consumer (D2C) and quick commerce model. The share of e-commerce in retail transactions is already large, and the development of GDP is an active catalyst, and the active online customers are more than 500 million. With this expansion, data consumption on the consumer behaviour is also grown drastically. Every online transaction will generate large amounts of personal data, such as names, addresses, telephone numbers, credit cards, browsing history, location, device fingerprinting, and behaviour clues.[1]

The e-commerce sites utilize this data to optimize supply chains, make use of dynamic pricing, detect fraud, do customized advertising, and personal recommendations. Such techniques enhance efficiency and convenience in corporations and leave multiple lasting digital footprints that could be disseminated, profiled, and sold.[2] Consequently, platforms possess greater technological and bargaining capability and in many cases, customers are providing their consent via lengthy privacy policies with limitations.[3]

Another important concern of consumers has also been realized in the form of data privacy. In Justice K.S Puttaswamy (Retd) Vs. Union of India the Supreme Court recognized informational privacy which is a key segment to the Article 21 right to life and personal liberty. This was a fundamental provision that made the State have to afford the correct protections. Nevertheless, introduction of it shows that there are serious problems, so the time to go and assess the lawmaking structure critically is timely and valuable.

Research Problem

Whether the legal system currently in force in India is sufficient to ensure consumer privacy in e-commerce or whether structural and enforcement loopholes still manifest the constitutional pledge of informational privacy.

[1] Organisation for Economic Co-operation and Development (OECD), Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013)
[2] Soumya Sharma and Chanjana Elsa Philip, Balancing E-Commerce and Data Privacy in India An Analytical Study, J. Info. Sys. Eng'g & Mgmt.
[3] Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion (2016)

ISSN: 2582-6433

Research Objective

To assess the sufficiency of the current Indian legal framework based on the privacy of data in e-commerce by defining and developing knowledge of particular regulatory loopholes in cross-border data flows, algorithmic personalization and profiling, and the principle of minimization of data under the DPDPA 2023, and assessing how these loopholes, along with the discontinuous interaction between the DPDPA and the Consumer Protection Act.

Methodology and Scope

The research is a doctrinal and comparative, policy-oriented research method. It is based mostly on the primary legal sources the Constitution of India, the Supreme Court rulings particularly the Puttaswamy case, the DPDP 2023, the DPDP Rules 2025, the IT Act 2000, and the CPA 2019/E-Commerce Rules 2020 supported by secondary literature and governmental notifications. The EU GDPR is selectively used to make comparisons with India to benchmark its approach. The critical analysis is based on the fact that it contrasts the framework with the constitutional values, international best practices, and consumer-protection imperatives. The target is carefully narrowed down to B2C e-commerce in India. It does not even enter other digital worlds or carry out major empirical field research, but makes use of available secondary data and doctrinal critique. It is a close methodology that allows a thorough analysis without compromising the fact that both law and technology are developing very fast.

Structure of the paper

The article is divided into seven sections. Section 2 gives an overview of both the constitutional and statutory framework. Section 3 is a critical study of major regulatory loopholes in cross-border transfers, algorithmic personalization, and data minimization. Section 4 analyzes the effect of such perforations on consumer trust and confidence. Section 5 contains comparative understanding of the GDPR and other jurisdictions. In section 6, specific policy and legal recommendations are provided. A conclusion on findings is given in Section 7.

Legal Framework

Constitutional Basis

The constitutional basis of the data privacy in India is well-established in the landmark ruling of the Supreme Court of Justice in the practice Justice K.S. Puttaswamy (Retd.) v. Union of

ISSN: 2582-6433

India (2017).[4] Based on a nine-judge bench ruling the Court considered that the right to privacy is an inherent aspect of the right to life and personal liberty of Article 21 of the Constitution and is bound to the provisions of equality of Article 14 and the freedoms of Article 19. In its ruling, informational privacy was expressly declared a fundamental part to this right, which stated that individuals became entitled to control what is gathered or used about them. Puttaswamy struck down all the previous restrictive precedents, like, M.P. Sharma Vs.Union of India[5] and Kharak Singh Vs. Union of India[6] and cemented the fact that privacy is not a negative restriction of State action, but a positive affirmation of the obligation of the State to create effective regulatory protections against both the state and non-state actors. This constitutional requirement becomes very important in the e-commerce scenario. Platforms openly handle sensitive personal and behaviour information on a regular basis to carry out commercial activities. Accordingly, the judgment forms the basis on which one can test the statutory framework in creating effective individual control over the personal data. whether any regime does not offer this guarantee, it stands a risk that it infringes on this constitutional assurance.

Evolution of Statutory Framework

Until 2023, e-commerce data privacy was not properly addressed in a differentiated and solid statutory framework. The case law of Information Technology Act, 2000[7] and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules)[8] was the cornerstone law. Section 43A made body corporate liable in civil proceedings in respect of failure to exercises reasonable security measures in respect of sensitive personal data or information (SPDI) whereas Section 72A entailed criminal penalties as a result of the illegal disclosure of information acquired through a legitimate contract. The SPDI Rules specified reasonable security practices and required consent in any of the situations where possible, yet only in a small group of sensitive data and without full rights, restriction on purposes, or specialized enforcement equipment.[9]

Prior to Digital Personal Data Protection Act, this framework was highly criticized

[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC
[5] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300
[6] Kharak Singh v. State of U.P., AIR 1963 SC 1295
[7] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India)
[8] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gaz. of India, Apr. 11, 2011, pt. II, sec. 3(ii) [hereinafter SPDI Rules]
[9] See SPDI Rules, r. 5–8

ISSN: 2582-6433

because it lacked individual rights and did not cater to the new threats including behaviour profiling and the cross-border transfers.[10] The Consumer Protection Act, 1986 subsequently substituted by the CPA 2019, was not forgiving to unfair trade practices but failed to consider data privacy as an independent consumer right.

Notified on 11 August 2023, the Digital Personal Data Protection act, 2023 (DPDPA)[11] operates by the Digital Personal Data Protection Rules, 2025[12] and there was a shift in paradigm. It substituted the previous practise of a piece meal advancement with a broad, accords-centre, cross sector regulation applicable to all digital personal data processing and having extra-territorial effects. The Act is based on the fiduciary model, where entities that decide the purpose and the ways of processing are Data Fiduciaries and individuals are Data Principals. This shift at the security regime into a rights-based regime is a result of the constitutional requirement of Puttaswamy and an attempt to strike a balance between individual autonomy and legitimate business needs in the digital economy.

Key Features of DPDP Act

DPDPA is rooted on seven core values transparency, limitation of purpose and minimization of the data, accuracy, restriction of storage, security provisions, and accountability. Section 5 provides that the consent must be free, definite, informed, unconditional, and unambiguous and it must be preceded by a clear standing notice. Data Principles can exercise rights of access, correction, erasure, withdrawal of consent and redressing grievances which are enforceable. Significant Data Fiduciaries(SDF) or large e commerce platforms that meet the set requirements, are assigned extra requirements including appointing Data Protection Officer, Data Protection Impact Assessment, and high-level security and audit. This is further imposed upon DPDP Rules, 2025 that further offer more in the form of detailed formats of notice, Consent Manager registration, breach-notification period, and long duration (three year) retention of big platforms which are also exempted. It has risk-based fines, with a maximum of 250 crore to an extreme violation, and is conducted by an independent Data Protection Board of India.

[10] Mahantesh B. Madiwalar & B.S. Reddy, Privacy Rights and Data Protection in Cyberspace with Special Reference to E-Commerce, Bharati L. Rev., Apr.–June 2017, at 71, 73
[11] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDPA]
[12] Digital Personal Data Protection Rules, 2025, notified by Ministry of Electronics & Information Technology, Gaz. of India, Nov. 13, 2025.

ISSN: 2582-6433

Interaction with Consumer Law

There is a two-layered regime wherein the DPDPA is effective to the Consumer Protection Act, 2019 (CPA) and the Consumer Protection (E-Commerce) Rules, 2020.[13] CPA and E-Commerce Rules necessitate the e-commerce websites to possess grievance officers, post their privacy policies and not indulge in unfair trade activities with the customer data. He or she also requires forums to protect the consumers against false claims and unnecessary redressing of grievances founded on data abuse. The tasks the marketplace actors are supposed to do under the E-Commerce Rules do not imply the extensive rights and fiduciary obligations in the DPDPA. This interface constitutes conflict. platforms must be actively utilizing both of these regimes, which causes conflict in grievance machines and precisely overlapping reporting, which may produce inconsistency in the norms of enforcement. The CPA nature of data protection also leans more toward lesser protection of such privacy breach, compared to the rights-oriented nature of the DPDPA, with the consumers remaining to negotiate a redressal path on a case-by-case scenario.[14] Overall, the legal framework has turned into a rights-based architecture instead of a focused and narrow security-centered model. Nevertheless, the reality that also coincides with consumer law. continued to exist and that the DPDPA remains at the initial developmental phases asserts that it does not sufficiently work in the e-commerce environment.

Key Regualatory Gaps in Indian Framework

Cross-Border Data Transfers

Section 17 of the DPDPA takes the model of a blacklist or negative-list of cross-border data transfers. Such personal data can be moved out of India to any other country or territory with the exception that the Central Government, by notification, limits such movement. This strategy constitutes a clear deviation to the tougher demands of data-localization of an earlier draft bill and would serve to liberalize the operations of e-commerce platforms based in other countries of the foreign cloud provider, advertising network and logistical partners.[15] The Act does not give clear criteria or methodology of adequacy assessment and public consultation process to include countries on the restricted list. Standard Contractual Clauses or Binding

[13] Consumer Protection Act, 2019, No. 35, Acts of Parliament, 2019 (India); Consumer Protection (E-Commerce) Rules, 2020, Gazette of India, July 23, 2020, pt. II, sec. 3(i)
[14] Mahantesh B. Madiwalar & B.S. Reddy, Privacy Rights and Data Protection in Cyberspace with Special Reference to E-Commerce, Bharati L. Rev., Apr.–June 2017, at 71, 78–80
[15] See Anupam Chander & Uyen P. Le, Data Nationalism, 64 Emory L.J. 677, 712–15 (2015) (discussing the uncertainties created by blacklist-style transfer regimes in emerging economies).

ISSN: 2582-6433

Corporate Rules are not mentioned in the DPDP Rules, 2025. Consequently, e-commerce organizations can no longer make any reliable forecasts on which jurisdictions will be abruptly constricted, and they cannot have a transfer system that is complete-proof.

Additionally, the blacklist model contradicts the localization requirements of stricter payment system data requirement of the Reserve Bank of India (RBI). Embedded finance or UPI-linked check out platforms are required to have two compliance architectures, which adds both costs and compliance friction. The lack of standardized tools of transfer is high in comparison with the strong adequacy determinations and contractual securities of the EU GDPR, where the information of Indian consumers to data stays unrestricted by the jurisdictions with weaker protections without any meaningful transparency or accountability.

Algorithmic Personalization

The third type of recommendation, applicable to a particular customer, is Algorithmic Personalization and Profiling. The regulatory vacuum is also in the total legislative silence concerning the matters of algorithmic personalization and behaviour profiling.[16]There are no statements in the DPDPA and DPDP Rules about automated decision-making, inferred data as well as taking initiative and using recommendation engines as per the dynamism of price or targeted advertising and credit rating. General obligations of consent and purpose restriction under the Sections 5, and section 8 provide indirect and insufficient protections.

Data Minimization

In section 6(1) of the DPDPA the principle of data minimization is codified, and it is stated that consent shall be limited to the necessary amount of personal data to achieve the purpose stated. The DPDP Rules enhance this by notices that are itemized and a granular consent requirement. Hypothetically, the principle opposes the trend of the culture of data maximization that commonly exists within digital markets. Theoretically, however, minimization is not much more than stem-and-line. Thousands of audits of the most popular platforms in 2025 show large-scale over-collection in the form of dark patterns and other unnecessary permission requests. Even when the actual application still needs only an elementary identity, many apps still collect clickstream and all manner of device data. Older SPDI Rules that were established to collect legacy datasets are usually processed based on

[16] Vikas Kathuria & Avirup Bose, Algorithmic Personalisation and Consumer Harm in India: A Regulatory Gap Analysis, 12 NUJS L. Rev. 1, 18–22

ISSN: 2582-6433

diverse old-fashioned consents, and this breaches the test of necessity. Mechanisms of enforcement are low. The Data Protection Board has just begun its activity, and no significant punishment has been chosen yet in particular, with the violations of minimization. Lack of quantitative necessity tests, sector specific checklists, and proactive audits enable platforms to judge themselves in respect of compliance at low risk.[17]

Regulatory Fragmentation

The DPDPA was a horizontal and multi-sector law. As a matter of fact, it co-exists with a winding net of sector regulations producing a lot of fragmentation. The Master Directions on Payment System Data, by the RBI, require financial data to be highly localized and have a period of retention, which is directly against the DPDPA more lenient approach to blacklist and its rights to erase.[18] On the same note, the IRDAI provisions require higher retention of insurance and health-related data whereas telecom regulations of TRAI introduce limits of consent and sharing in case of OTP-based authentication. Grievance officers and privacy policies are a requirement of both the Consumer Protection Act, 2019 and Consumer Protection (E-Commerce) Rules, 2020, where segment of the law takes data protection as a subsidiary to overall consumer rights, not as a fundamental right itself.[19] They charge small and medium enterprises (SME) and D2C brands, who do not have privacy teams, disproportionately. The lack of a formal inter-regulatory coordination mechanism results into disparities in enforcement, regulatory arbitrage and confusion to consumers. A transaction conducted through e-commerce when money is paid, insurance is added, and the product is delivered may lead to the strains of four regimes.

Effect on Market Behaviour and Consumer Trust

The regulatory gaps that were found in the previous section are not in a vacuum. They have a direct relationship with actual damage to consumer confidence and disrupted market behaviour within the e-commerce environment in India. Although informational privacy was enshrined in the constitution and the introduction of the DPDPA, the weak enforcement show and ad-hoc solutions to the problem remain and undermine the belief of people in doing transactions online.

[17] Pratiksha Baxi & Namita Wahi, Data Minimisation and Enforcement Challenges under the DPDPA, 45 Econ. & Pol. Wkly. 45, 48–51
[18] Shruti A. Bhandary, Data Localisation and Cross-Border Data Flows: The Indian Experience, 15 Indian J. L. & Tech. 89, 102–05 (2019)
[19] Mahantesh B. Madiwalar & B.S. Reddy, Privacy Rights and Data Protection in Cyberspace with Special Reference to E-Commerce, Bharati L. Rev., Apr.–June 2017, at 71, 78–80.

ISSN: 2582-6433

Data Breaches and Payment Frauds

Cyber attacks on high-profile data and the sudden increase in the number of cases of payment frauds have become the most accessible icons of the lack of trust in online commerce. BigBasket, Zomato and Flipkart are among some of the major platforms that have been impacted by incidents that expose millions of records with names, addresses, phone numbers and payment details. Such violations are usually caused by insufficient security protection and data archiving overboarding Payments fraud has become even more critical.rn. Under the influence of the extensive use of UPI, about a quarter of Indian families that operate in the field of digital payment fell victims of phishing, SIM swapping, or fraudulent transactions. Numerous accidents are never reported because of intimidation or lack of faith in redresses.[20]

Weak Consumer Remedies

The Consumer Protection Act, 2019 (CPA) and the Consumer Protection (E-Commerce) Rules, 2020 were to enhance the consumer protection through the requirements of the e-commerce platforms to have grievance officers, post transparent privacy policies and disclose unfair trade practices involving data. Nonetheless, these provisions have made data protection as an appendage to general rights of consumers as opposed to fundamental rights. The outcome is minimalist solutions.[21] Although the CPA does offer a system of complaints in front of Consumer Commissions, it does not have the deep knowledge and prompt reaction capabilities that the Data Protection Board brings out under the DPDPA. Redressal channels are usually parallel where consumers are left with no choice but to use channel A and B especially when it concerns data-related grievances. The auxiliary rank of privacy in the CPA implies that breaches do not receive the severe repercussions that one could have under the DPDPA, further weakening accountability.[22]

Behavioural Consequences

The accumulative impact of breaches, frauds and inadequate remedies is quite obvious in the change in the consumer behaviour. The experience of empirical research and industry publications all indicate higher cart abandonment rates, much higher adoption of cash-on-delivery (COD) instead of electronic payment, and more frequent switching between risk-

[20] Vikas Kathuria & Avirup Bose, Algorithmic Personalisation and Consumer Harm in India: A Regulatory Gap Analysis, 12 NUJS L. Rev. 1, 18–22 (2024).
[21] LocalCircles, Dark Patterns and Over-Collection of Data in Indian E-Commerce Platforms: 2025 Audit Report 12–15 (2025)
[22] Pratiksha Baxi & Namita Wahi, Data Minimisation and Enforcement Challenges under the DPDPA, 45 Econ. & Pol. Wkly. 45, 48–51 (2025)

ISSN: 2582-6433

averse customers. The bulk of consumers are now confined to only critical purchases or do not submit any sensitive data especially those in the upper two cities in Tier-2/Tier-3 groups who are first-time buyers or simply less digitally engaged. This is further warned by dark patterns and privacy practices. Consumers usually become manipulated instead of being empowered when they are presented with long consent forms or pre-checked boxes in response to marketing activities. The lack of trust deteriorates into a decrease in repeat purchases, the willingness to use personalized recommendations, and the rate of adoption of new e-commerce features. In platforms, this change in behaviour raises the cost of acquisition of customers and limits the ability to get revenues through data-based advertising. At a macro level, it endangers the inclusive digital development as it dishearten the vulnerable groups to fully engage in the digital economy.

Comparative Perspectives

General Data Protection Regulations

The General Data Protection Regulation (GDPR) of the European Union, which has been in operation since 2018, provides a practical comparative prism through which the failures of the DPDPA can be assessed. The GDPR is more prescriptive and rights-centre and directly overcomes most of the loopholes in the Indian framework. Consent should be granular, free and as easy to revoke as it is to grant it, and data minimization should be provided by obligatory Data Protection Impact Assessment (DPIA) and Privacy by Design (Article 25).[23] The GDPR, too, has strong cross-border transfer instruments ie, adequacy decisions, Standard Contractual Clauses, and Binding Corporate Rules, which are much more legally sure than the Indian blacklist strategy.. These characteristics have proven to increase the standards of compliance as well as consumer trust in the digital market within the EU.

India: Structural and Economic Differences

Although the GDPR offers many useful ideas, the direct transplantation to India is impossible and undesirable. The economic and structural reality of India is contrasted with the European reality. Having a big e-commerce sector that is heavily dominated by SME and D2C, high digital-divide pressures, and the necessity to encourage quick digital inclusion, an excessively prescriptive regime might cause excessive compliance expenses and innovation stifling. The model of the GDPR presupposes the presence of mature supervisory institutions and high rates

[23] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1, arts. 13–15, 22, 25.

ISSN: 2582-6433

of digital literacy which are not yet fully developed in India, as the Data Protection Board is at its infancy, and most consumers in Tier-2/3 cities are unfamiliar with the notion of data rights. A more balanced solution should be sought, that is, maintaining the loose, consent-based basis of DPDPA but with specific protections that will help mitigate the particular dangers of Indian e-commerce.[24]

Legal Reforms

To begin with, the Central Government should come up with clear and transparent regulations regarding cross-border data transfers. The existing blacklisting system under Section 17 ought to be complemented with objective adequacy standards, compulsory Standard Contractual Clauses and a process of public consultation prior to restrictions being notified. This would minimize uncertainty among the e-commerce platforms and offer substantial protection to Indian consumers, whose information is exported to foreign countries. Second, the DPDPA should specifically identify the evils of algorithmic personalization and profiling. Transparency obligations, right to explanation and opt-out mechanism on significant automated decisions (such as dynamic pricing or targeted advertising) should be introduced by a new provision. E-commerce sector-specific codes of practice ought to be announced to ban manipulative dark patterns and to impose impact assessment of high-risk profiling systems. These reforms would fill the regulatory vacuum that is present and would bring the law closer to the informational privacy requirement of Puttaswamy.

Institutional Strengthening

The weakest point in the current regime is the enforcement. Data Protection Board of India should be operational with proper staffing, technological set-ups and e-commerce desks. It should exercise proactive audit powers, conduct frequent reviews of compliance of Significant Data Fiduciaries, and the ability to issue binding codes of practice.[25] The fragmentation of the regulations is a significant hindrance. An Inter-Regulatory Coordination Committee with the Data Protection Board, RBI, IRDAI, TRAI, and Central Consumer Protection Authority should be made permanent so that they can come up with common guidelines and solve disputes. The Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020 are

[24] Mahantesh B. Madiwalar & B.S. Reddy, Privacy Rights and Data Protection in Cyberspace with Special Reference to E-Commerce, Bharati L. Rev., Apr.–June 2017, at 71, 78–80.
[25] Shruti A. Bhandary, Data Localisation and Cross-Border Data Flows: The Indian Experience, 15 Indian J. L. & Tech. 89, 102–05 (2019).

ISSN: 2582-6433

to be revised to match the rights-centered model of the DPDPA, removing the redundant grievance processes and establishing a single-window redressal system in the system of consumer protection.

Consumer Centre Measure

Lastly, the issue of consumer empowerment has to be emphasized. The digital literacy campaigns on a nationwide level should be based on the rights to data, the management of consent, and the awareness of dark patterns.[26] These reforms would be legal, institutional, harmonization and consumer-centre, and would turn the DPDPA into a strong, enforceable regime. Plugging the pinpointed gaps, India will be able to create a trusted e-commerce environment that neither undermines the constitutional promise of informational privacy nor innovation.[27]

Conclusion

The present paper has established that India has a familiar legal protection of data privacy in e-commerce, which is based on the constitutional acknowledgement of informational privacy in Puttaswamy (2017) and implemented by the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025. The DPDPA brought about the concept of consent-based, fiduciary and risk-based penalties, which is a significant improvement to the previous piecemeal regime of the IT Act and SPDI Rules. The framework is however not complete. There are still critical regulatory loopholes in cross-border data transfers (ambiguous blacklist approach), algorithmic personaliation and profiling (total silence in legislation), data minimization (theory-practice gap), and inter-regulatory harmonization with the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020

References

1. *Organisation for Economic Co-operation and Development (OECD), Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013)*

[26] Vikas Kathuria & Avirup Bose, Algorithmic Personalisation and Consumer Harm in India: A Regulatory Gap Analysis, 12 NUJS L. Rev. 1, 18–22 (2024).
[27] LocalCircles, Dark Patterns and Over-Collection of Data in Indian E-Commerce Platforms: 2025 Audit Report 12–15 (2025)

ISSN: 2582-6433

2. *Soumya Sharma and Chanjana Elsa Philip, Balancing E-Commerce and Data Privacy in India An Analytical Study, J. Info. Sys. Eng'g & Mgmt.*
3. *Federal Trade Commission, Big Data: A Tool for Inclusion or Exclusion (2016)*
4. *Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC*
5. *M.P. Sharma v. Satish Chandra, AIR 1954 SC 300*
6. *Kharak Singh v. State of U.P., AIR 1963 SC 1295*
7. *Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India)*
8. *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Gaz. of India, Apr. 11, 2011, pt. II, sec. 3(ii) [hereinafter SPDI Rules] See SPDI Rules, r. 5–8*
9. *Mahantesh B. Madiwalar & B.S. Reddy, Privacy Rights and Data Protection in Cyberspace with Special Reference to E-Commerce, Bharati L. Rev., Apr.–June 2017, at 71, 73 Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDPA]*
10. *Digital Personal Data Protection Rules, 2025, notified by Ministry of Electronics & Information Technology, Gaz. of India, Nov. 13, 2025.*
11. *See Anupam Chander & Uyen P. Le, Data Nationalism, 64 Emory L.J. 677, 712–15 (2015) (discussing the uncertainties created by blacklist-style transfer regimes in emerging economies).*
12. *Vikas Kathuria & Avirup Bose, Algorithmic Personalisation and Consumer Harm in India: A Regulatory Gap Analysis, 12 NUJS L. Rev. 1, 18–22*
13. *Pratiksha Baxi & Namita Wahi, Data Minimisation and Enforcement Challenges under the DPDPA, 45 Econ. & Pol. Wkly. 45, 48–51*
14. *LocalCircles, Dark Patterns and Over-Collection of Data in Indian E-Commerce Platforms: 2025 Audit Report 12–15 (2025)*
15. *Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1, arts. 13–15, 22, 25.*