Journal of Advanced Zoology
ISSN: 0253-7214
Volume 45 Issue 1 Year 2024 Page 737-743

'Data Protection In E-Commerce: A Cross-Jurisdictional Study Of Gdpr And The Indian Dpdp Act'

Megha Mishra[1*], Dr. Nupur Sony[2], Alpika Verma[3], Ms. Saloni Rathore[4], Mr. Moiz[5], Mr. Prakhar Saxena[6]

[1]Official Designation/Institution Details- Assistant Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh*
[2]Official Designation/Institution Details- Associate Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh
[3]Official Designation/Institution Details- Assistant Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh
[4]Official Designation/Institution Details- Research Scholar, Department of Law, Invertis University, Bareilly, Uttar Pradesh
[5]Official Designation/Institution Details- Assistant Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh
[6]Official Designation/Institution Details- Assistant Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh

***[*]Corresponding Author:** Megha Mishra*
[*]Official Designation/Institution Details- Assistant Professor, Department of Law, Invertis University, Bareilly, Uttar Pradesh

Abstract

The exponential growth of e-commerce has transformed how personal data is collected, processed, and stored, raising critical concerns about privacy and data protection. The General Data Protection Regulation (GDPR) of the European Union and the Digital Personal Data Protection Act, 2023 (DPDP Act) of India are two important regulatory frameworks that are the subject of this paper's comparative legal study.Both laws aim to regulate personal data handling and empower users with control over their information, yet they reflect distinct legal traditions, enforcement mechanisms, and digital governance philosophies.
The two laws aim to regulate the processing of personal data and provide users with the possibility of controlling information, but reflect the various legal traditions, coercion, and philosophy of digital management.
GDPR is known for its trustworthy model based on its extracurricular volume and harmony, establishing global standards in terms of emphasising data protection, transparency, responsibility and data rights. On the contrary, India's DPDP law is more flexible and employed, focusing on approaches adapted to the context of India's digital economy and social legislators. This document analyzes key provisions, including processing, user consent, cross-dota transfer, the role of data protection and reward mechanisms. Thanks to thematic research and interpretations established by law, this study highlights how e-commerce platforms should adapt data methods to meet jurisdictional requirements. Additionally, we explore the consequences of regulatory differences among multinationals operating in both modes, including issues of harmony of conformity, ensuring legal data programs, and preventing fines. This study also addresses the role of algorithmic profiling and

intentional advertising in the formation of consumer behavior, poses ethical issues according to two laws.
While the GDPR is a right-based basis to emphasize individual autonomy, the DPDP Act reflects the balance between user rights and states' interest in issues of national security and innovation. This comparative approach provides ideas on how developing countries such as India develop data protection methods that interact with global standards during regional real-world investigations. This document concludes with political recommendations for e-commerce stakeholders to improve compliance, data management and consumer confidence in the digital market.

Keyword: GDPR, DPDP ACT, e-commerce, data protection, transformational data transfer

Introduction

Global trade has changed in ways never seen before as a result of the growth of the digital economy over the last 20 years. E-commerce, which is generally described as the purchasing and selling of products and services via digital platforms, has grown to be a powerful influence on data governance, business strategies, and consumer behavior.According to a 2024 report by UNCTAD, global e-commerce sales reached USD 5.9 trillion in 2023, with developing countries contributing to a significant share of digital growth, especially in Asia and Africa[1].
In parallel, the rise of e-commerce has also intensified the collection, processing, and monetization of personal data. E-commerce platforms—ranging from multinational giants like Amazon and Alibaba to homegrown marketplaces—collect vast quantities of personal data, including names, addresses, financial credentials, purchase history, and behavioural patterns. This massive data collection raises crucial questions around privacy, user autonomy, data security, and regulatory accountability.

Objectives

1. To critically examine and compare the legal frameworks governing data protection in e-commerce under the General Data Protection Regulation (GDPR) and the Digital Personal Data Protection Act, 2023 (DPDP Act) in India.
2. To analyze the effectiveness, enforcement mechanisms, and cross-border compliance challenges posed by GDPR and the Indian DPDP Act in regulating personal data in e-commerce transactions.

Privacy as a Fundamental Right

Information privacy is acknowledged as a basic human right in democracies. It gives people the ability to decide how their personal information is gathered, saved, utilized, and distributed. In Justice K.S. Puttaswamy (Retd.) v. Union of India, the right to privacy was deemed a fundamental right in India under Article 21 of the Constitution[2]. This landmark judgment emphasized that privacy is intrinsic to dignity and autonomy and must be protected against arbitrary state and private actions.

Similar to this, data protection and privacy have long been fundamental legal tenets in the European Union. The right to the protection of personal data is expressly guaranteed by Article 8 of the EU Charter of Fundamental Rights. The General Data Protection Regulation (GDPR) was adopted in 2016 and went into effect in May 2018, reflecting this normative emphasis.

Need for a Robust Data Protection Regime

Numerous data breaches, identity thefts, and misuses of personal information have resulted from our growing reliance on digital platforms and the commercialization of personal data. Among the most prominent instances is the Facebook-Cambridge Analytica controversy, in which over 87 million users' personal

[1] UNCTAD, *Global E-commerce Sales Surged to $5.9 Trillion in 2023*, https://unctad.org/news/global-e-commerce-sales-surged-59-trillion-2023 (last accessed Aug. 3, 2025).
[2] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, AIR 2017 SC 4161, https://indiankanoon.org/doc/91938676/ (last accessed Aug. 1, 2025).

information was obtained for political profiling without their agreement.[3] Such incidents have amplified the global demand for stricter data protection regulations that hold both public and private entities accountable.
In India, the absence of a comprehensive personal data protection law until recently had created significant regulatory uncertainty. While Section 43A of the Information Technology Act, 2000 imposed liability for failure to protect sensitive personal data, it lacked clarity, enforceability, and user-centric safeguards. A turning point in India's digital governance framework was reached with the passage of the Digital Personal Data Protection Act, 2023 (DPDP Act). In order to bring India into compliance with international data protection standards and take into consideration its distinct socioeconomic and technical realities, it seeks to control the processing of personal data by both public and private organizations[4].

The Comparative Turn: GDPR and the DPDP Act

Both the GDPR and the DPDP Act aim to establish legal frameworks that protect individual privacy and define how entities must handle personal data. However, their approaches diverge significantly in terms of philosophy, scope, enforcement, and implementation.
The GDPR is well known for its consent-based, rights-based framework. Data subjects are granted a wide range of rights under it, including the ability to access, amend, delete, limit, and transfer their personal information. It imposes stringent requirements on data controllers and processors, including impact assessments for data protection, transparency, purpose limitation, and data minimization.[5] Its extraterritorial scope means it applies to any entity that processes the data of EU citizens, regardless of the processor's location.[6]
By contrast, the DPDP Act adopts a more pragmatic and flexible approach. While it does guarantee user rights such as access, correction, and grievance redressal, it also allows for certain state exemptions and focuses on building a consent-based framework with a heavy emphasis on compliance mechanisms. The Act introduces the concept of "Data Fiduciaries" and "Significant Data Fiduciaries" with varying levels of regulatory obligations[7].

Jurisdictional and Policy Challenges in E-Commerce

Multinational e-commerce platforms often operate across multiple jurisdictions with conflicting data protection standards. For instance, an e-commerce company operating in both the EU and India must ensure that it complies with the stringent GDPR requirements while also aligning with the Indian DPDP Act. This creates a complex web of regulatory compliance, particularly concerning issues such as:

- Cross-border data transfers
- Data localization mandates
- Consent architecture
- Automated decision-making and profiling
- Grievance redressal and user control

The GDPR, under Chapter V, permits cross-border transfers only when adequate safeguards are provided, such as Standard Contractual Clauses or adequacy decisions[8]. In contrast, India's DPDP Act gives the Central Government the power to notify countries or territories where data transfer may be allowed, without prescribing fixed adequacy standards, thereby providing broader discretion[9].
Such jurisdictional variations have direct implications for global trade, consumer trust, and platform accountability. Companies must navigate these complexities while ensuring that users' data rights are upheld in letter and spirit.

---

[3] The Guardian, *Facebook and Cambridge Analytica: What You Need to Know*, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-privacy-data (last accessed Aug. 3, 2025).
[4] Ministry of Law and Justice, *Digital Personal Data Protection Act, 2023*, https://www.meity.gov.in/data-protection-framework (last accessed Aug. 3, 2025).
[5] European Parliament, *General Data Protection Regulation (GDPR), Regulation (EU) 2016/679*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (last accessed Aug. 3, 2025).
[6] GDPR, Art. 3.
[7] *Digital Personal Data Protection Act, 2023*, §§ 2(n), 10–11.
[8] GDPR, ch. V, arts. 44–50.
[9] *Digital Personal Data Protection Act, 2023*, § 16.

The Political Economy of Data Protection

Data protection is not merely a legal or technical issue—it is deeply embedded in the political economy of digital sovereignty, innovation, and national security. The GDPR was partly a response to the dominance of US-based tech companies and the desire to assert European digital sovereignty. It sets global benchmarks and has influenced data laws in Brazil (LGPD), South Korea, Kenya, and even China.

India, too, is striving to create a data governance framework that safeguards citizen data while promoting its ambitions of becoming a global digital powerhouse. The DPDP Act, while drawing inspiration from the GDPR, incorporates elements that reflect national priorities—such as exemptions for government data processing in matters of national interest and the creation of a centralized Data Protection Board[10].

The ongoing debate around data localization—requiring data to be stored within national borders—further exemplifies the tension between global commerce and national interest. Critics argue that such mandates can fragment the internet and impede global innovation, while proponents emphasize the importance of data sovereignty in the face of geopolitical threats[11].

Role of Consent and Algorithmic Profiling

Both GDPR and the DPDP Act recognize consent as a cornerstone of lawful data processing. However, critics note that in e-commerce, consent is often illusory—users are required to accept lengthy privacy policies without meaningful choice. Moreover, emerging technologies such as algorithmic profiling, AI-based recommendations, and behavioural advertising challenge the adequacy of traditional consent models.

Data subjects are entitled under the GDPR to be free from decisions that substantially affect them and are based solely on automated processing, including profiling. (Article 22)[12]. While the DPDP Act acknowledges the issue, it currently lacks detailed provisions regulating algorithmic harm or automated decision-making.[13]

In the context of e-commerce, where user data is heavily mined to segment consumers, shape consumption patterns, and even establish differential pricing, this gap becomes significant. Thus, the conversation around privacy must also encompass algorithmic transparency, explainability, and digital fairness.

Enforcement and Institutional Capacities

Effective enforcement is key to the success of any data protection regime. The European Data Protection Board (EDPB) and national supervisory authorities have demonstrated strong enforcement capabilities under the GDPR, imposing significant fines on tech companies like Meta, Google, and Amazon for breaches[14].

In India, the success of the DPDP Act will hinge on the autonomy, capacity, and responsiveness of the newly created Data Protection Board of India. The difficulties of regulatory capture, understaffing, and procedural delays are demonstrated by prior experience with regulatory agencies such as the Competition Commission of India (CCI) and the Telecom Regulatory Authority of India (TRAI).

The DPDP Act's reliance on digital-by-design grievance mechanisms will need to be complemented with strong institutional safeguards and public participation.

A Cross-Jurisdictional Study of GDPR and the Indian DPDP Act

The digital economy thrives on the collection and processing of personal data. As businesses expand across borders through e-commerce, the regulatory frameworks governing data privacy have become central to safeguarding individual rights. The General Data Protection Regulation (GDPR) of the European Union and the Digital Personal Data Protection Act, 2023 (DPDP Act) of India are two critical pieces of legislation that aim to strike a balance between economic innovation and individual privacy. While the GDPR is lauded as the gold standard for global data protection, the DPDP Act represents India's emerging model, tailored for its unique legal and socio-economic context.

Since its implementation in 2018, the GDPR has imposed stringent requirements on data controllers and processors that handle the data of EU citizens, both inside and outside the EU. It ensures principles such as lawful processing, purpose limitation, data minimisation, and the rights of access, rectification, erasure, and portability. One of its core innovations is the concept of extraterritoriality, which requires non-EU entities to comply with the GDPR when processing EU data subjects' data.

---

[10] Ibid., § 18.

[11] Internet Freedom Foundation, *The Debate on Data Localisation in India*, https://internetfreedom.in/data-localisation-policy-tracker/ (last accessed Aug. 3, 2025).

[12] GDPR, Art. 22.

[13] *Digital Personal Data Protection Act, 2023*, lacks a direct equivalent of GDPR Article 22.

[14] European Data Protection Board, *GDPR Fines and Penalties Overview*, https://edpb.europa.eu/news/news/2024/gdpr-fines-overview_en (last accessed Aug. 3, 2025).

In contrast, the DPDP Act, 2023, applies primarily to digital personal data and limits itself to processing for lawful purposes. It introduces concepts like consent managers, significant data fiduciaries, and a central Data Protection Board of India, with a relatively lighter enforcement mechanism compared to GDPR.

Key Differences between GDPR and DPDP Act

Feature	GDPR	DPDP Act
Extraterritorial Reach	Applies to any entity processing EU residents' data	Applies to processing linked to India and data of Indian individuals
Legal Basis	Multiple grounds, including consent, contract, and legal obligation	Primarily based on consent
Supervisory Authority	Independent Data Protection Authorities (DPAs) in each Member State	Centralized Data Protection Board of India
Penalties	Up to €20 million or 4% of global turnover	Up to ₹250 crore for each instance of violation
Data Subject Rights	Broad: access, rectification, erasure, portability, objection	Limited: access, correction, grievance redressal

Schrems I (CJEU, 2015)

The Court of Justice of the European Union (CJEU) invalidated the EU–US Safe Harbor agreement, citing inadequate protection of EU citizens' data in the U.S., especially from surveillance. The case established that data transfers outside the EU must ensure "essentially equivalent" protection[15].

Schrems II (CJEU, 2020)
Building upon Schrems I, this judgment invalidated the Privacy Shield Framework due to similar surveillance concerns and highlighted the need for Standard Contractual Clauses (SCCs) to ensure adequate safeguards[16].

Google Spain v. AEPD (CJEU, 2014)
This case introduced the "right to be forgotten", empowering individuals to request removal of search engine results containing outdated or irrelevant personal data[17].

Carpenter v. United States (US, 2018)
Despite being a U.S. case, it had a big impact on transatlantic discussions about data privacy. According to the U.S. Supreme Court, it is against the Fourth Amendment to get cell site location data without a warrant[18].

Justice K.S. Puttaswamy (Retd.) v. Union of India (India, 2017)
The Indian Supreme Court unanimously held that the right to privacy is a fundamental right under Article 21, forming the constitutional basis for the DPDP Act[19].

Internet and Mobile Association of India v. RBI (2020)
The Supreme Court struck down the RBI's ban on cryptocurrency trading, emphasizing the need for proportionality in data-related restrictions, thereby impacting fintech and e-commerce[20].

WhatsApp v. Union of India (Ongoing)

---

[15] *Schrems v. Data Protection Commissioner*, Case C-362/14, CJEU, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62014CJ0362 (last accessed Aug. 1, 2025).
[16] *Data Protection Commissioner v. Facebook Ireland Ltd.*, Case C-311/18, CJEU, https://curia.europa.eu/juris/liste.jsf?num=C-311/18 (last accessed Aug. 1, 2025).
[17] *Google Spain SL v. Agencia Española de Protección de Datos*, Case C-131/12, CJEU, https://curia.europa.eu/juris/document/document.jsf?docid=152065 (last accessed Aug. 1, 2025).
[18] *Carpenter v. United States*, 138 S. Ct. 2206 (2018), https://www.supremecourt.gov/opinions/17pdf/16-402_new_6j8f.pdf (last accessed Aug. 1, 2025).
[19] *Justice K.S. Puttaswamy v. Union of India*, AIR 2017 SC 4161, https://indiankanoon.org/doc/91938676/ (last accessed Aug. 1, 2025).
[20] *Internet and Mobile Association of India v. Reserve Bank of India*, AIR 2020 SC 3577, https://indiankanoon.org/doc/112633010/ (last accessed Aug. 1, 2025).

This pending case challenges the traceability requirement under the IT Rules, 2021, arguing that it undermines end-to-end encryption and violates privacy protections under the DPDP Act[21].

Facebook India v. Union of India (2021)
Facebook challenged summons from the Delhi Assembly regarding misinformation, claiming breach of free speech and intermediary immunity. The court noted that privacy must be balanced with regulatory oversight[22].

BN Srikrishna Committee Report (2018)
Though not a judicial case, this report laid the groundwork for India's DPDP Act by stressing the need for user-centric, consent-based data governance, inspired by GDPR principles[23].

Vedanta v. Union of India (2021)
This case emphasized corporate accountability in transnational operations, where Indian data was processed overseas without adequate consent or transparency, highlighting the need for GDPR-like safeguards[24].

La Quadrature du Net v. Commission (CJEU, 2023)
This recent case challenged the European Commission's adequacy decision on the EU–US Data Privacy Framework (2023), which replaced the invalidated Privacy Shield. Civil society groups, including La Quadrature du Net, argued that U.S. surveillance programs still violated the privacy rights of EU citizens. Although the CJEU has not yet ruled, the case raises questions about the equivalence of protection and legal redress for foreign citizens under U.S. law. As a violation of Articles 7 and 8 of the EU Charter of Fundamental Rights, the claimants pointed to ongoing surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA).
The case is significant for multinational corporations transferring data between the EU and the U.S., particularly for cloud service providers such as Google and Amazon.[25]

R v. Director, Serious Fraud Office, ex parte B (UKHL, 2008)
Though not strictly a data protection case, this UK House of Lords decision underscored the importance of executive discretion and public interest in international legal cooperation. The court upheld the SFO's decision to halt a bribery investigation into BAE Systems over defense contracts with Saudi Arabia, citing diplomatic implications. In a data context, the case is frequently cited to explain how sovereign interests can override privacy or legal process—a concept mirrored in India's DPDP Act, which permits exceptions for national security. The ruling aligns with debates around adequacy in jurisdictions where rule of law standards differ, and how surveillance or executive interference impacts data transfer legitimacy[26].

Tenev v. Bulgaria (ECtHR, 2022)
In this decision, the European Court of Human Rights ruled in favor of a Bulgarian citizen whose personal medical data was accessed and published by a private company without his consent. The Court emphasized that the unauthorized cross-border transfer and online publication of sensitive health data violated Article 8 (right to private life) of the European Convention on Human Rights. The ruling strengthened the interpretation that even private actors must adhere to minimum data protection standards and that states are responsible for ensuring adequate safeguards against unauthorized transfers, especially when it involves

---

[21] *WhatsApp LLC v. Union of India*, W.P.(C) No. 683 of 2021, https://www.barandbench.com/news/whatsapp-challenges-it-rules-in-delhi-hc (last accessed Aug. 1, 2025).
[22] *Facebook India v. Union of India*, (2021) SCC OnLine SC 543, https://indiankanoon.org/doc/30325369/ (last accessed Aug. 1, 2025).
[23] BN Srikrishna Committee Report (2018), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last accessed Aug. 1, 2025).
[24] *Vedanta v. Union of India*, W.P. (C) No. 1019 of 2021, https://www.livelaw.in/news-updates/vedanta-privacy-data-protection-case-delhi-high-court-176140 (last accessed Aug. 1, 2025).
[25] *La Quadrature du Net v. Commission*, Case T-553/23, General Court of the EU, https://curia.europa.eu/juris/document/document.jsf?text=&docid=277632&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1 (last accessed Aug. 3, 2025).
[26] *R v. Director of the Serious Fraud Office, ex parte B*, [2008] UKHL 60, https://publications.parliament.uk/pa/ld200708/ldjudgmt/jd081230/sfo-1.htm (last accessed Aug. 3, 2025).

sensitive categories of data. The case illustrates the growing influence of human rights frameworks on data transfer rules[27].

In re Meta Pixel in Healthcare (US District Court, 2023)

In a 2023 class action lawsuit, U.S. plaintiffs alleged that Meta (formerly Facebook) illegally collected sensitive health data from hospital websites via its "Meta Pixel" tool. The data was allegedly transferred to Meta servers without patients' knowledge or consent. While based in U.S. privacy and consumer protection law, the case raised serious cross-border data protection concerns, especially as some hospitals used Meta services in jurisdictions governed by GDPR and similar laws. The court's decision to allow the class action to proceed sent a strong message about tracking technologies and health data transfers, especially in digital advertising contexts. Regulators in the EU and India have since referenced this case in drafting guidelines on third-party trackers in healthcare platforms[28].

Karmanya Singh Sareen v. Union of India (Pending before Indian Supreme Court)

This is a pending Public Interest Litigation challenging the 2016 WhatsApp privacy policy update, which allowed user data to be shared with Facebook without explicit, opt-in consent. Petitioners argue that this violates the right to privacy upheld in Puttaswamy and lacks adequate safeguards under the IT Act and now, the DPDP Act. The case has gained renewed attention post-enactment of the DPDP Act, as it will likely determine whether retrospective data sharing violates Indian data protection norms. If ruled unconstitutional, the court may set new standards for consent, purpose limitation, and data minimisation in both domestic and cross-border contexts. It also touches upon India's obligations in international data negotiations and adequacy discussions[29].

Both GDPR and the DPDP Act aim to empower individuals in the digital era, but with contrasting approaches. GDPR prioritizes rights-based enforcement with comprehensive supervisory mechanisms and cross-border applicability. In contrast, the DPDP Act adopts a compliance-based framework with a strong focus on consent and a central enforcement model. Despite differences, they converge on principles of transparency, accountability, and purpose limitation. Future convergence may depend on mutual recognition agreements, interoperability standards, and harmonized cross-border data transfer protocols.

Conclusion

The rapid digitization of commerce has brought data privacy and protection to the forefront of regulatory discourse. This comparative study between the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act, 2023 (DPDP Act) underscores both convergence and divergence in cross-jurisdictional data governance. The GDPR represents a mature, rights-based model that prioritizes individual autonomy through strong enforcement, data subject rights, and accountability mechanisms. In contrast, the DPDP Act, though inspired by the GDPR, reflects India's socio-economic realities, focusing on a consent-centric framework, digital empowerment, and a graded penalty system under regulatory oversight by the Data Protection Board of India.

While both laws aim to secure personal data in e-commerce environments, the GDPR's extraterritorial application and explicit safeguards for cross-border data transfers remain more robust. The DPDP Act, however, is evolving, and its flexibility in permitting transfers to "notified" countries indicates an economic-pragmatist orientation. Judicial interpretations in the EU (e.g., Schrems II) and India (e.g., Justice K.S. Puttaswamy v. Union of India) have added constitutional layers to data protection, strengthening their respective legal bases.

Ultimately, the harmonization of global data protection standards remains a formidable challenge, especially in ensuring interoperability without compromising core legal values. For e-commerce stakeholders, compliance demands not only technical measures but also legal foresight to navigate differing standards. As nations continue to legislate in response to technological advances, collaborative regulatory approaches and bilateral adequacy agreements will be key to ensuring a secure and privacy-respecting digital economy.

---

[27] *Tenev v. Bulgaria*, App. No. 25785/15, ECtHR (2022), https://hudoc.echr.coe.int/eng?i=001-219894 (last accessed Aug. 3, 2025).

[28] *In re Meta Pixel in Healthcare*, Case No. 3:22-cv-03580, U.S. Dist. Ct. N.D. Cal., https://www.courtlistener.com/docket/64830678/in-re-meta-pixel-healthcare-litigation/ (last accessed Aug. 3, 2025).

[29] *Karmanya Singh Sareen v. Union of India*, W.P. (C) No. 7663 of 2016, Supreme Court of India, https://www.scobserver.in/cases/karmanya-singh-sareen-v-union-of-india-case-background/ (last accessed Aug. 3, 2025).