QUBAHAN POLITICAL JOURNAL
VOL. 5, NO. 1, February 2026
https://doi.org/10.48161/qpj.v5n1a41

# Legal Compliance and Consumer Protection in the Digital Marketplace: GDPR-Driven Standards for E-Commerce Privacy Policies within the International Legal Framework

**Madhulika Singh [1], Tatiana Suplicy Barbosa[2]**

[1]Faculty of Law, Jai Narain Vyas University, 342011, India.
[2]Departments of Law and Psychology, UniFael – Centro Universitário, Lapa, Paraná, Brazil.

* **Corresponding author:** madhulikasingh200@gmail.com.

**ABSTRACT:** The foundation of European Union's General Data Protection Regulation (GDPR), has played a pivotal role in regulating rapid digitalization of global commerce, bringing in the necessary model shift in digital data governance. The article explores in depth GDPR as a transnational regulatory instrument crucial in enforcing extraterritorial reach of its provisions. Further the Court of Justice of the European Union (CJEU) have through judicial activism and expansive interpretation defined corporate digital responsibility. The article highlights how transcontinental regulation, especially through the 'Brussels Effect', GDPR has transformed privacy into a competitive differentiator, through play in market dynamics rather than being enforced through stringent legislations. The article then moves to study the pressure of GDPR's requirement for autonomous consumer consent and corporate dark patterns that slyly bypasses the regulatory hammer of data sovereignty. The celebrated cases against Meta and Amazon are analysed to illustrate the transition of privacy policies from symbolic disclosures to enforceable legal instruments. Furthermore, the article provides a comparative evaluation of India's Digital Personal Data Protection (DPDP) Act, 2023, highlighting the normative convergence between the 'rights-based' European model and India's 'sovereignty-driven' framework. The cross-national development on the regulation of privacy is emerging, though structural divergences regarding state exemptions and regulatory independence remain the persistent challenges. The article suggests a 'highest common denominator' compliance strategy and a shift toward 'privacy by design' to navigate this increasingly fragmented international legal landscape.

**Keywords:** GDPR, DPDP Act 2023, brussels effect, E-commerce law, data sovereignty, consumer protection.

## I. INTRODUCTION

### *1. DATA, DIGITAL MARKETS, AND CONSUMER VULNERABILITY*

The data being the fuel to the digital economy is crucial to complete not only the transaction at hand, but also to predict consumer preferences, personalization of interface and the shaping of consumer's consumption behaviour through algorithmic positioning of products. The said functionalities of consumer data not only make it an economic asset, but also makes it susceptible to consumer vulnerability. The e-commerce giants lay a systematic web to extract, process, and monetize personal data. The exponential growth of cross-border e-commerce has transformed personal data into a central commodity of the global digital economy. While the personal data fuels the digital economy, it often stands in logger heads with the consumer privacy and informational autonomy. Thus, the regulatory bodies across the jurisdictional regimes increasingly conceptualize data protection as an integral dimension of consumer protection.

The traditional consumer protection legislations fall flat in the digital economy age, for they are ill equipped to address harms arising from opaque data practices, asymmetrical information flows, and behavioural manipulation.[1] Therefore to fill up the regulatory gap between the current data manipulation and outdates legal mechanism, cross border legislations have emerged with data protection law as a complementary and increasingly fundamental pillar of consumer protection in digital markets.

The European Union's General Data Protection Regulation (GDPR), is one of its kind to highlight the revolutionary concepts of extraterritoriality, imposition of hefty fines and sanctions that older laws lacked. Unlike earlier privacy frameworks, GDPR embeds consumer-centric principles such as transparency, fairness, accountability, and autonomy into legally enforceable obligations.[2] The extraterritorial scope of the Regulation, is not a nascent concept, GDPR's predecessor, EU's Data Protection Directive of 1995 too had extraterritorial scope but lacked the teeth to enforce it. GDPR further extend these norms to compel global e-commerce platforms to internalize privacy protection standards regardless of their physical location.

The article tries to take in the view of GDPR-driven e-commerce privacy standards within the broader international legal framework and examines their implications for cross-border consumer protection. It further evaluates the influence of GDPR on India's Digital Personal Data Protection Act, 2023 (DPDP Act), highlighting areas of convergence, divergence, and the persistent regulatory tension in global digital commerce.

The article is developed in the following structure: Section II provides a literature review of the consumer privacy debate, contextualizing the shift from physical to digital surveillance. Section III details the Material and Methodology, adopting qualitative doctrinal approach combined with a comparative legal analysis of international treaties and regional statutes. Section IV provides jurisdictional data analysis, where the article critically evaluates the current legal standing and enforcement mechanisms in the European Union and India. Lastly section V concludes with a three-pronged global recommendation.

## II. RELATED WORK

The digital commerce has brought about a transcendental shift from moving from a view of data as a mere byproduct of communication to what is now commonly termed the fuel of the global digital economy. To understand the development of privacy as a fundamental human right, the article majorly draws from Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR). Contemporary scholarship highlights positive obligation of the state to protect consumer rights in the digital sphere, The Brussels Effect (Anu Bradford, 2012 & 2023) has elaborately discussed upon the phenomenon of Brussels Effect, where GDPR has been adopted across the jurisdictions, not through treaties but market mechanisms. Virtual Competition (Ezrachi & Stucke, 2016) submits that the algorithms facilitate collusion and price discrimination, undermining consumer welfare. Data Protection Law in India (Rahul Matthan, 2022) and Digital Privacy and India's DPDP Act (Shyam Divan, 2023) helps navigate through comparative analysis between the EU's independent and right based framework vis-à-vis the Indian model that balances individual rights with national security and executive discretion. Furthermore, The Trade Origins of Privacy Law (Anupam Chander, 2024) suggests that modern privacy regimes are increasingly used as tools of trade diplomacy, where the adequacy of a nation's data laws dictates its participation in the global digital economy.

## III. MATERIAL AND METHOD

This section outlines the orderly methodology adopted to appreciate and analyse the intersection of consumer privacy protection and digital commerce. Given the nature of study, the research adopts a qualitative doctrinal approach combined with comparative legal analysis to evaluate the efficiency of current regulatory frameworks.

### *1. DATA COLLECTION*

- Primary Sources: the primary sources of data consist of the international and national statutes, EU General Data Protection Regulation (GDPR), India Digital Personal Data Protection (DPDP) Act, 2023. International

treaties and conventions, namely The Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) and landmark judicial pronouncements.

- Secondary Sources: the secondary sources include academic literature, which includes but is not limited to, The Brussels Effect by Anu Bradford, Virtual Competition by Ezrachi & Stucke, Data Protection Law in India by Rahul Matthan. Articles from the International Data Privacy Law and the Journal of European Consumer and Market Law are consulted to map the trajectory of contemporary legal debates. Publications of international bodies such as regarding the United Nations Guidelines for Consumer Protection (UNGCP), amongst other policy briefs.

### *2. RESEARCH DESIGN*

The present research is structured as a qualitative doctrinal study, focusing on the legislative framework and how it is being interpreted to meet the exigencies of consumer data and privacy protection in digital economy age. The qualitative component involves analysis of privacy policies and user interface standards, through the course of research the sociological and economic impact of deceptive data gathering techniques is observed and how it impacts the consumer autonomy is studied. The second element to research design is the comparative legal methodology to compare the European 'Rights-Based' model with the Indian 'Sovereignty-Driven' framework. The study aims not just to analyse the legislative structure of both the jurisdiction but to unfold the practical operationalities in achieving the common goal of consumer data and privacy protection in digital landscape.

## IV. DATA ANALYSIS

This section is a systematic analysis of the primary and secondary sources to decode the legislative frameworks, specifically the European Union's GDPR and the Indian Digital Personal Data Protection (DPDP) Act. The analysis progresses methodically, firstly the paper elucidates upon the foundation of digital privacy, secondly, the evolution of GDPR as global solution is postulated to fill up the enforcement gap left by the predecessor soft laws. Thirdly the discourse moves to unfold the dark patterns employed by the digital commerce companies and evaluates the regulatory response. Fourthly the research moves to comparative analysis between the EU's right based approach and India's sovereignty driven paradigm. Lastly the cross jurisdictional enforcement challenges are synthesised.

### *1. PRIVACY AS A FUNDAMENTAL HUMAN RIGHT AND THE DIGITAL SHIFT*

Privacy as a fundamental right is well established in international law and all major jurisdictions. With the advent of digital age, the same right has now an extended dimension of digital privacy. International recognition of privacy as a fundamental right clearly precedes the digital economy, yet the relevance of this right has arguably never been more pronounced than in today's data-driven markets. To understand the implication of digital privacy, it will be helpful to view privacy not as a static right, but as an evolving boundary between the self and the external world.

Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibit arbitrary or unlawful interference with an individual's privacy, family, home, or correspondence.[3][4] These provisions date back to era when surveillance was majorly through physical and state centric modes, and the circulation of the any such information was in limited form. In today's digital age the regulatory essence, of protecting individuals from intrusive power has been adapted to suit digital realities.

The UN Human Rights Committee has played a significant role in this interpretative expansion. In its General Comments, the Committee has emphasized that the obligation to protect privacy is not limited to abstaining from interference but also requires states to adopt positive legislative and regulatory measures.[5] The multinational digital giants have access to vast amounts of consumer data, including but not limited to their names, locations, browsing habits, payment details, and behavioral patterns, most often in ways that consumers neither fully understand nor essential have control of,[6] therefore, requiring the interference of legislative and regulatory bodies much more than ever before.

The concerns of privacy violation in context of e-commerce are no longer mere technical compliance failure rather are a potential human rights concern. Viewing from an international human rights perspective, unchecked corporate data practices can undermine individual dignity just as effectively as unlawful state surveillance. [7] Algorithmic profiling and targeted advertising, now standard features of cross-border e-commerce, can influence consumer choices, reinforce existing biases, and restrict access to information.[8] Protection of one's privacy, especially in today's open digital market space, upon liberal interpretation, is closely tied to other fundamental rights, such as freedom of expression, equality, and non-discrimination.

The journey of consumer protection has evolved from tangible harm, i.e. defective goods, misleading advertisements, or unfair contract terms to intangible data leaks and unauthorised usage, thereby creating a transparency gap in consumer law. In cross border digital commerce, the harm is not caused by the product itself, but is ingrained in the choice architecture. The harm is not caused or experienced immediately, but is a future risk, as single instance of data collection may seem harmless, but the aggregation of that data across platforms allows the digital commerce platform for digital stalking and algorithmic positioning of products impacting consumer choices.

The United Nations Guidelines for Consumer Protection (UNGCP) acknowledge these emerging challenges. While originally adopted to address conventional consumer issues, the Guidelines have been updated to reflect the realities of electronic commerce and digital transactions. [9] UNGCP provides normative guidance, but a significant hurdle remains that it lacks binding legal force, thereby creating a 'compliance vacuum' that global digital platforms often exploit. The probability of exploitation and regulatory gap exemplifies when transaction is between parties subject to different legal regimes. When data misuse occurs, questions of applicable law, jurisdiction, and enforcement quickly complicate the possibility of effective redressal.[10]

Owing to the enforcement gap, GDPR rose to address the pertaining issue particularly significant in in the realm of cross-border e-commerce, extending its extraterritorial reach. By its applicability to non-EU entities that offer goods or services to EU consumers, GDPR effectively exports its consumer protection logic beyond Europe. [11] The extraterritorial grasp of GDPR, has partially filled the regulatory vacuum created by the absence of binding international consumer protection norms for digital markets.

In the digital markets, although the broader trend of digital consumer protection is quite clear, the consumers outside EU may not enjoy the same level of protection or access to remedies, even when interacting with the same platforms. Therefore, making the responsibility of at least the developed and developing jurisdictions to imbibe stringent provisions of consumer protection in digital realm, into their regulatory system.

## *2. GDPR AS A TRANSNATIONAL REGULATORY INSTRUMENT: THE BRUSSELS EFFECT*

The General Data Protection Regulation (GDPR) came into force in 2018. Its development was part of a decades-long evolution of privacy law. The regulation today stands as a stout support to further strengthen not just European legislative framework, but also as a dominant global benchmark for data privacy. The extraterritorial reach of GDPR has enabled to address the friction that exists between the global nature of data flows and the territorial nature of legal jurisdiction. Concomitantly, another particular phenomenon called 'Brussels Effect' [11] is analysed to understand how GDPR's consumer privacy standards are adopted globally through market mechanisms.

GDPR principles have made a paradigm shift in how consumer privacy is perceived in global digital markets. The extraterritorial reach makes it possible to influence the legal and operational architectures of foreign jurisdictions. The digital companies adhere to consumer protection policies not as a legislative mandate, but as a prerequisite for international market participation.[12]

GDPR through Article 3, and along with other legislations i.e. EU AI Act (2024) and the EU Data Act (2025) has established transnational 'privacy constitution'. Article 3 establishes two main criteria for its applicability. Firstly, the 'Establishment Criterion' it applies to processing of personal data in the context of the activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union or not. Second is the 'Targeting Criterion', which applies to controllers and processors not established in the EU where processing activities relate to the offering of goods or services to data subjects in the Union or the monitoring of their behavior within the Union.

The interesting phenomenon that has transcended the EU's boundaries and has been readily adopted by digital commerce giants, is called the 'Brussels Effect'. The term was coined by Anu Bradford, it describes the adoption of strict standards for privacy not through treaties but as a prerequisite to match international market competition. The Brussels Effect thrives when global companies find it economically inefficient to maintain different standards for different regions.

The 'Brussels Effect' influences the global market through two distinct paths. First is the de facto adoption, which is voluntary corporate adoption of GDPR standards, to streamline operations. Second is the de jure adoption, wherein countries like Brazil, India, and Japan model their national laws on the GDPR, to facilitate smoother cross-border data flow.[13]

The reach of GDPR's standards is affirmed and expanded by Court of Justice of the European Union (CJEU). CJEU has moved beyond merely interpreting the GDPR, to bridging the gap between consumer law and data protection by actively weaponizing it as a tool for consumer empowerment. The two ruling that laid the ground work for 'right to be forgotten' under Article 17 GDPR, and correct definition of consumer 'consent', have been discussed below.

In Google Spain SL v AEPD (2014) [1], the Court established that a search engine operator could be considered a 'controller' and that its activities were sufficiently linked to an EU establishment (the Spanish subsidiary) to trigger EU law. This case laid the groundwork for the 'Right to be Forgotten', Art. 17 GDPR. This case established that an individual has the right to request that search engines 'de-index' links to information that is 'inadequate, irrelevant or no longer relevant', 'de-link' thereby means that the information that fall in the latter criterion is not deleted from the internet entirely, but is removed from search results, forming the basis of Article 17 of the GDPR.

Another significant ruling, Planet49 GmbH (2019 [2] decisively impacted the global e-commerce user experience. The CJEU clarified that 'consent' must be active and digital commerce modalities like pre-ticked boxes for cookies or marketing are invalid. It was ruled that consent is not 'freely given' or 'specific' if it is obtained through silence, inactivity, or pre-selected boxes.

### *3. GDPR'S REGULATORY BATTLE AGAINST DARK PATTERNS IN E-COMMERCE*

The global commerce chains have blurred the national regulatory boundaries, the loop holes in the system give way to deceptive user interface (UI) and user experience (UX) designs that deliberately mislead, coerce, or manipulate consumers into making choices they wouldn't have otherwise made.[14] The misleading strategies used by the global digital commerce giants are structured to extract personal data, undermining the principle of freely given consent.

The access to consumer data, fuels the running of multinational digital commerce companies, due to regulatory gap the economy thrived on friction-less acquisition of user data. With bridging of this gap between the data protection and consumer law, the era of unfettered data harvesting has now come to an end. Therefore, now the digital commerce companies have resorted to manipulating consumer behaviour by introducing dark pattern, ranging from 'forced action' to 'emotional steering' for extraction of data from consumer interaction, posing fundamental thereat to integrity of data protection.

According to the GDPR standard of 'consent', it must be freely given, specific, informed, and unambiguous. In the context of e-commerce, this requires a clear affirmative action. Article 4(11) and Article 7 explains the same. The dark pattern unfolds in one or more of the following ways to deceive the consumer from making an informed decision, deceptive practices include, but are not limited to the following ways;

- Subscription trap: wherein the digital platform makes it easier to sign up, but almost impossible to cancel the subscription;
- False urgency: fake countdown timers are placed to play with customers psychology.
- Drip pricing: is introduced which hides the taxes, service charges until the final checkout screen.
- Basket sneaking: is placed by platforms to add extra item to the cart, without consumer's consent.
- Overloading: Repeatedly prompting for consent, until the consumer clicks it, just to clear the screen
- Privacy maze: Designing the interface so that the 'accept all' button is prominent while the 'reject all' or 'settings' options are hidden in sub-menus
- Stirring: using a language that makes the user feel guilty or foolish for rejecting the private option and not disclosing his/her personal details.

In addition to the forementioned principles and fundamental requirement of freely given consent, the GDPR provides comprehensive framework of the following articles to ensure that the dark patterns are not leveraged to cheat the user;

- Article 12: upholds the requirement of clear and plain language, and is increasingly interpreted by CJEU to be against legalistic complication. In the 2024 Meta inquiries, regulators emphasized that the 'transparency gap' the distance between what a user think is happening and what the technical processing entails must be bridged by the interface itself. [15]
- Article 25: The principle of Data Protection by Design, requires platforms to integrate privacy into the core architecture of their systems. In e-commerce, this means that the most privacy-friendly settings, e.g., no behavioural tracking, must be the default. Any departure from this state must be a deliberate, uncoerced choice of the user. [16]

## *4. COMPARATIVE ANALYSIS OF THE GDPR AND INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023*

This section aims to explore the convergence between India's Digital Personal Data Protection (DPDP) Act, 2023, and the global 'gold standard' of the EU's GDPR. This subsection undertakes to explore how both aim to reduce the regulatory gap. Although both frameworks strive to achieve the universal goal of consumer privacy protection, yet diverge in functional parameters owing to the jurisprudential difference.

While the DPDP Act adopts the GDPR's core principles of consent, purpose limitation, and accountability, it diverges significantly in its treatment of state exemptions, regulatory independence, and cross-border transfer mechanisms. It is interesting to note that when GDPR came in force in 2018, India too had planted the seeds of privacy as a fundamental right. The Indian Supreme court in the case of Justice K.S. Puttaswamy v. Union of India, laid the foundational ground work for DPDP Act.

There exist a few shared principles on which both the jurisdictions converge. The DPDP Act reflects a clear GDPR influence in its structural terminology and principles. What the GDPR terms 'Data Subjects' and 'Data Controllers', the DPDP Act labels 'Data Principals' and 'Data Fiduciaries' [17]. Both frameworks centre on the following aspects;

- Consent-Centric Processing: Requiring consent to be free, informed, specific, and unambiguous.
- Purpose Limitation and Data Minimization: Restricting collection to what is necessary for the specified intent.
- Accuracy and Accountability: Placing the burden on entities to maintain data integrity and document compliance.

India being one of the world's largest digital markets, through DPDP Act has imbibed a few shared principles with GDPR, yet has several structural divergences from it as well. India's sovereignty driven departures from GDPR may have significant implications for global e-commerce.[18] Following are the distinctions from GDPR;

- State Exemptions and Executive Discretion: One of the most contentious areas of the DPDP Act is Section 17, which provides broad exemptions for the state. While the GDPR (Recital 16 and Art. 2) allows for national security and law enforcement exemptions, these are strictly governed by the principles of necessity and proportionality in a democratic society.[19] In contrast, the DPDP Act allows the Central Government to exempt any 'instrumentality of the State' from the Act's core provisions in the interest of sovereignty, integrity, or public order.[20] The debate intensifies here as, this creates a 'bifurcated privacy regime' where corporate actors are strictly regulated, but state surveillance remains largely sheltered.
- Regulatory Architecture: Independence vs. Control: The GDPR mandates that supervisory authorities be completely independent from government influence (Art. 52). The Indian model, however, states that the Data Protection Board of India (DPBI), established under DPDP Act, is a body appointed and structurally governed by the Central Government; raising concerns about its ability to act as a truly independent body to check on state-linked data fiduciaries. [21]
- Cross-Border Data Transfers: Adequacy vs. Blacklisting: GDPR Model uses 'whitelist' approach, i.e. data can flow freely to countries deemed to have 'adequate' protection (Art. 45 of GDPR), or through Standard Contractual Clauses (SCCs). The DPDP Model adopts blacklist approach (section 16 of DPDP Act) the data transfer is permitted to all jurisdictions except those specifically restricted by government notification; this

approach may be more business-friendly in the short term, it creates uncertainty as the criteria for 'blacklisting' remains undefined and prone to political sensitivity. [17]

- EU's 'Right to be Forgotten' to India's 'Correction and Erasure': Under Article 17 of the GDPR, the 'Right to be Forgotten'/ 'Right to Erasure' allows data subjects to demand deletion of their personal data without undue delay under specific conditions.[1] These include circumstances where the data is no longer necessary for its original purpose, the subject withdraws consent, or the data has been processed unlawfully. Contrastingly the DPDP Act frames the right more broadly but also more restrictively; wherein a Data Fiduciary must erase personal data upon receiving a request unless its retention is 'necessary for the specified purpose or for compliance with any law'. This clause 'compliance with any law' is wider in scope than the GDPR's exceptions, potentially allowing for longer data retention periods if mandated by sectoral Indian regulations.

### *5. CROSS JURISDICTIONAL ENFORCEMENT AND CHALLENGES*

The rising digital landscape has encountered glitches rooted in jurisdictional limitations. GDPR has set standard of conduct with its comprehensive rights framework and penalty regime. Yet the effectiveness rests with the enforcement bodies of each country. The inherent nature of e-commerce involving multiple stakeholders, furthermore all situated in different jurisdictions often exposes the consumer privacy to a 'protection vacuum' where traditional territorial laws fail to provide adequate redressal. The ambiguity of delay and latches in the consumer protection, expose individual consumers to unlawful data practices for extended periods without effective remedies. Moreover, individual customers rarely have the resources to pursue cross-border complaints independently, making institutional enforcement the primary mechanism for rights realization.

To address these challenges, GDPR introduced a cooperative enforcement architecture centred on the 'one-stop shop' mechanism, under which a lead supervisory authority coordinates enforcement for cross-border processing activities. [22] While this model may be theoretically appealing, achieving its objectives of reducing regulatory fragmentation and ensuring consistency in decision-making in cross border remained farfetched. Further the model was condemned for procedural delays, resource disparities among national data protection authorities and jurisdictional disputes over lead authority competence. [23]

The complexities further tighten for stakeholders in countries where national data protection legislations are in place. GDPR here acts as an additional layer of legal complexity. The digital platform, consumer or the seller enterprises may be subjected simultaneously to both the national data protection/consumer protection laws and GDPR. Overlapping regulatory regimes not only entails increased legal compliance costs but also poses strategic uncertainty, particularly where standards diverge or enforcement expectations differ. [24] This uneven access highlights a structural imbalance in global consumer protection, where rights are formally universal but substantively uneven in their application.

Strengthening cooperation between regulatory authorities, enhancing access to cross-border remedies, and fostering greater convergence between data protection and consumer law frameworks are essential steps toward addressing the jurisdictional challenges of the digital marketplace. [25] Despite the challenges enumerated above GDPR's cross-border enforcement model has exerted significant normative influence. Jurisdictions across the world are now proactively designing their domestic consumer privacy law in sync with international consumer privacy standards.

## V. CONCLUSION

To resolve the 'protection vacuum' in the digital commerce space, created by multiple stakeholders situated in different jurisdictions, it will be practical to move beyond simple legal adherence and adopt corporate digital responsibility. The same can be implemented through adoption of following suggestions which are designed to bridge the gap between national sovereignty and the borderless nature of digital commerce as we move through this digital age.

- Adoption of 'Fairness-by-Design': by the logic of this principle the companies will be under an obligation to eliminate deceptive choice architecture and fulfil the transparency mandate as a prerequisite for market entry. The companies can be mandated to establish internal 'Ethics Boards' to audit algorithms for dark

patterns and price discrimination before deployment. The privacy polices should be easy to understand by the consumer, moving away from the 'black box' models.

- Strengthening Cross-Border Redressal Mechanisms: digital platforms can integrate independent, third-party Online Dispute Resolution (ODR) mechanisms that operate across jurisdictions. Another step can be made towards Mutual Recognition Agreements, through which cross jurisdictional regulatory setups recognize each other's data protection certifications, simplifying the compliance burden for small and medium enterprises (SMEs).
- Adopting Highest Common Denominator (HCD) Strategy: this strategy suggest shift from a niche legal theory to a core operational necessity for global e-commerce. It suggests that if a digital commerce company complies by the mandate of GDPR, which is one of world's toughest privacy standards, it will automatically comply with 90% of any new laws passed in other jurisdictions. Further for applicability to other countries with special jurisdictional requirement, HCD can be 'layered' with local mandate of the country.

The evolution of consumer data protection law has remarkably developed from 2016 to 2026, where not just the multinational e-commerce giants are adopting data privacy protocols, but also the regulatory gaps are being systematically filled.

However, the comparative analysis with India's DPDP Act reveals a growing tension with the rise of digital sovereignty. While India has embraced the normative principles of the GDPR (consent, minimization, and transparency), it has also asserted a state-centric model that prioritizes national security and executive discretion over the absolute independent oversight favoured by the EU in GDPR. This suggests that while the language of privacy is becoming universal, its application still remains subject to geopolitical realities. For the international legal framework to remain effective, it must continue to bridge the gap between high-level rights and the technical realities of the global e-commerce ecosystem.

## FUNDING STATEMENT

This research received no external funding.

## CONFLICTS OF INTEREST

The authors declare no conflicts of interest

## REFERENCES

1. *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, Case C-131/12, ECLI:EU:C:2014:317, May 2014.
2. *Planet49 GmbH v. Bundesverband der Verbraucherzentralen*, Case C-673/17, ECLI:EU:C:2019:801, Oct 2019.
3. UN General Assembly, "Universal Declaration of Human Rights," GA Res. 217A (III), UN Doc. A/810, Dec. 10, 1948.
4. UN General Assembly, "International Covenant on Civil and Political Rights," Dec. 16, 1966, United Nations Treaty Series, vol. 999, p. 171, Mar. 23, 1976.
5. UN Human Rights Committee, "General Comment No. 16: Article 17 (Right to Privacy)," UN Doc. HRI/GEN/1/Rev.9, 1988.
6. R. Á. Costello, *Critical Reflections on the EU's Data Protection Regime*. Oxford University Press, 2024.
7. UN General Assembly, "The Right to Privacy in the Digital Age," UN Doc. A/RES/68/167, 2013.
8. S. Wachter, B. Mittelstadt, and L. Floridi, "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation," *International Data Privacy Law*, vol. 7, no. 2, pp. 76–99, 2017.
9. UNCTAD, "United Nations Guidelines for Consumer Protection," United Nations Conference on Trade and Development, 2016.
10. C. Busch, "Digitalisation and the law of consumer contracts," *Journal of European Consumer and Market Law*, vol. 11, no. 1, pp. 12–25, 2019.
11. A. Bradford, "The Brussels effect," *Northwestern University Law Review*, vol. 107, no. 1, p. 1, 2012.
12. A. Chander, *The Trade Origins of Privacy Law*. Cambridge University Press, 2024.
13. M. D. Birnhack and G. Mundlak, "The Brussels effect(s) and the rise of a privacy profession," *International Data Privacy Law*, vol. 15, no. 2, pp. 138–155, 2025.
14. European Data Protection Board, "Guidelines 03/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them," Apr. 2023.
15. European Commission, "Commission preliminarily finds Meta in breach of transparency obligations under the Digital Services Act," Press Release IP/24/2503, Oct. 2024.

16. European Data Protection Board, "Guidelines 4/2019 on Article 25 Data Protection by Design and by Default," Oct. 2020
17. A. Yadav and R. Pandey, "Data privacy across borders: A comparative analysis of European Union and Indian protection laws," *University of Bologna Law Review*, vol. 10, no. 1, pp. 177–210, 2025.
18. R. Matthan, *Data Protection Law in India*. Oxford University Press, 2022.
19. G. Greenleaf, "The DPDP Act 2023: India's compromised step toward data privacy," *Privacy Laws & Business International Report*, vol. 182, pp. 1–6, 2023.
20. S. Divan, "Digital privacy and India's DPDP Act," *Journal of Indian Law and Society*, vol. 14, no. 1, pp. 45–68, 2023.
21. A. Bradford, *Digital Empire: The Global Battle to Regulate Technology*. Oxford University Press, 2023.
22. *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)*, 2016 O.J. (L 119) 1.
23. European Data Protection Supervisor, "Opinion on the functioning of the One-Stop-Shop mechanism," 2021.
24. A. Burman, "India's new data protection law: The good, the bad, and the unknown," Carnegie India, Aug. 2023.
25. M. Burri, "The governance of data and data flows in trade agreements," *Journal of World Trade*, vol. 51, no. 3, pp. 407–425, 2017.