Page 2490 - 2499 **DOI:** *https://doi.org/10.63108/IJLMH.12745*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

The Intersection of the Digital Personal Data Protection Act, 2023, and Consumer Rights

MADHU NAGAR[*] AND DR. AYUSHI DUBEY[**]

ABSTRACT

The rapid expansion of India's digital economy has necessitated a robust and comprehensive legal framework to govern the rights of its citizens, particularly in the context of personal data and commercial transactions. The enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act), marks a watershed moment, establishing a legal right to data privacy for the first time. This paper analyzes the critical inter section of the DPDP Act with the existing Consumer Protection Act, 2019 (CPA), and its associated regulations, such as the Guidelines for Prevention and Regulation of Dark Patterns. The study argues that this intersection creates a complex, dual-layered regulatory framework that significantly strengthens consumer rights by elevating data privacy violations to the status of unfair trade practices. Key areas of convergence include the principle of informed consent, where deceptive design practices (dark patterns) violate both the DPDP Act's requirement for "free, specific, informed, and unconditional" consent and the CPA's prohibition on unfair trade practices. The paper further explores the potential for jurisdictional overlap and conflict between the newly established Data Protection Board (DPB) and the Central Consumer Protection Authority (CCPA), particularly concerning dual grievance redressal mechanisms and the conflict between the right to erasure and mandatory record retention. By examining legal precedents, including the foundational judgment and recent CCPA enforcement actions, the paper concludes that a holistic, integrated compliance approach is essential for businesses, while coordinated regulatory guidance is necessary to ensure effective and consistent protection of the digital consumer.

Keywords: *Digital Personal Data Protection Act 2023, Consumer Protection Act 2019, Consumer Rights, Data Privacy, Dark Patterns, Digital Autonomy, Unfair Trade Practice*

I. INTRODUCTION

The digital transformation of the Indian economy has brought with it unprecedented opportunities for commerce and innovation, simultaneously introducing new vulnerabilities for the individual consumer. As transactions migrate from physical market places to complex digital ecosystems, the consumer's identity and personal data have become inextricably linked to their commercial activity. This paradigm shift has necessitated a corresponding evolution in the legal

[*] Author is an Assistant Professor at IES University, Bhopal, India.
[**] Author is an Assistant Professor at IES University, Bhopal, India.

 [ISSN 2581-5369]

safeguards designed to protect the individual. In this context, the Digital Personal Data Protection Act, 2023 (DPDP Act), and the Consumer Protection Act, 2019 (CPA), form the twin pillars of digital governance in India.

The DPDP Act, rooted in the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*,[1] which declared privacy a fundamental right, is India's first comprehensive law dedicated to governing the processing of digital personal data. It establishes clear rights for the Data Principal (the individual) and corresponding obligations for the Data Fiduciary (the entity processing the data). Concurrently, the CPA 2019, with its focus on preventing Unfair Trade Practices (UTP) and protecting consumers from misleading advertisements and defective services, has been adapted to address the nuances of the digital space, notably through the establishment of the Central Consumer Protection Authority (CCPA).

The intersection of these two statutes is not merely incidental; it is a deliberate and crucial development in Indian jurisprudence. While the DPDP Act secures the informational privacy of the individual, the CPA ensures commercial fairness and autonomy in the marketplace. The central thesis of this paper is that the convergence of these two regulatory regimes creates a powerful, synergistic framework where violations of data privacy can be simultaneously construed as violations of consumer rights, thereby providing the digital consumer with a dual layer of protection and recourse. This paper will analyze the specific points of convergence and conflict, the implications for digital businesses, and the challenges posed by the dual enforcement structure.

II. The Regulatory Landscape: DPDP Act and CPA

To understand the intersection, a clear delineation of the scope and objectives of each Act is necessary.

A. The Digital Personal Data Protection Act, 2023

The DPDP Act is built on seven core principles, which collectively define the rights of the Data Principal and the duties of the Data Fiduciary. The most pertinent for consumer rights are:

- Principle of Lawful, Fair, and Transparent Processing: Data must be processed lawfully, fairly, and with transparency to the Data Principal.
- Principle of Purpose Limitation: Personal data can only be used for the purpose for which the Data Principal has given consent.

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

 [ISSN 2581-5369]

3 .Principle of Data Minimisation : Only the minimum amount of data necessary for the stated purpose should be collected.

- Principle of Accuracy: Data Fiduciaries must ensure the data is accurate and complete.
- Principle of Storage Limitation: Data must be deleted once the purpose of processing is served.
- Principle of Reasonable Security Safeguards: Technical and organisational measures must be implemented to prevent data breaches.
- Principle of Accountability: Data Fiduciaries are responsible for compliance and must be able to demonstrate it.

Crucially, the Act mandates that consent must be "free, specific, informed, unconditional and unambiguous" [2]. This stringent standard for consent forms the primary bridge between data privacy and consumer autonomy.

B. The Consumer Protection Act, 2019

The CPA 2019, which replaced the 1986 Act, introduced significant changes to address the digital age. It expanded the definition of "consumer" to include online transactions and established the CCPA to regulate matters relating to violations of consumer rights, unfair trade practices, and misleading advertisements.

The CCPA's power to investigate and act against Unfair Trade Practices (UTP) is the key mechanism through which it addresses digital harms. A UTP is defined broadly to include any practice that, for the purpose of promoting the sale, use, or supply of any

goods or services, adopts any unfair method or unfair or deceptive practice. In the digital context, this definition has been powerfully leveraged to combat manipulative design.

C. The Critical Link: The Dark Patterns Guidelines

The most explicit link between the two Acts is forged by the Guidelines for Prevention and Regulation of Dark Patterns, 2023, issued by the CCPA [3]. These guidelines classify thirteen specific deceptive design practices— such as 'False Urgency,' 'Basket Sneaking, "Confirm shaming,' and 'Forced Action'— as Unfair Trade Practices.

[2] The Digital Personal Data Protection Act, 2023, No. 22 of 2023, s. 6(1) (India).
[3] Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023* (30 November 2023) (India).

 [ISSN 2581-5369]

The classification of dark patterns as UTPs under the CPA is a direct intervention into the realm of data privacy. Many dark patterns are designed specifically to subvert the consumer's will to obtain personal data or consent for data processing. For instance, a 'Forced Action' pattern that requires a user to share their contact list to access a purchased service violates the DPDP Act's principle of data minimisation and purpose limitation, while simultaneously constituting an Unfair Trade Practice under the CPA by coercing the consumer into an action they did not intend. This dual exposure is a powerful deterrent for digital businesses.

III. The Nexus of Privacy and Consumer Autonomy

The intersection of the DPDP Act and the CPA is most pronounced in the concept of digital autonomy, which is undermined by deceptive practices and strengthened by the right to informed consent.

A. Consent as the Cornerstone of Digital Autonomy

The DPDP Act's definition of valid consent is central to consumer protection. When a Data Fiduciary employs a dark pattern to secure consent, that consent is rendered invalid under the DPDP Act because it is neither "free" nor" unconditional." The Act explicitly requires consent to be" free, specific, informed, unconditional and unambiguous" [4]. Dark patterns, by their very nature, introduce conditions, obfuscate information, or coerce the user, thereby vitiating the fundamental requirement of free consent. This is a direct attack on the consumer's digital autonomy.

For example, a 'Subscription Trap' that makes it extremely difficult to unsubscribe or requires unnecessary personal data (like payment details for a free trial) violates the DPDP Act on multiple fronts:

- Invalid Consent: The initial consent for the trial is not "free" if the exit mechanism is obscured or made intentionally cumbersome. The difficulty in withdrawing consent is equivalent to the consent not being freely given in the first place.
- Data Minimisation: Requiring payment details for a free service, even if only for verification, violates the principle of data minimisation, as the data collected is not strictly necessary for the stated purpose of providing a free trial. This practice also increases the risk profile for the Data Principal unnecessarily.

[4] Supra note 2.

 [ISSN 2581-5369]

- Right to Erasure: Making it difficult to exit the service effectively impedes the Data Principal's right to withdraw consent and request erasure of their data, a core right under the DPDP Act.

Furthermore, other dark patterns listed in the CCPA guidelines also have profound privacy implications. 'Pre-ticked Boxes' directly violate the requirement for specific and unambiguous consent, as the user's action is passive rather than affirmative. 'Nagging'— the persistent asking for personal data or permissions— can wear down a user's resistance, leading to consent that is not truly informed or freely given. In the context of the DPDP Act, any data processing that results from these manipulative techniques is unlawful, opening the Data Fiduciary to significant penalties.

By classifying such manipulative practices as UTPs, the CPA provides an additional, immediate layer of recourse. The CCPA can take action, issue directions to discontinue the practice, and impose penalties, effectively treating the subversion of data privacy rights as a form of commercial fraud against the consumer. This dual regulatory approach ensures that the consumer is protected not just from the misuse of data, but from the means by which the data was acquired.

B. Dark Patterns as a Dual Violation

The legal peril for businesses engaging in dark patterns is the exposure to simultaneous liability under both Acts. The following table illustrates how specific dark patterns can trigger violations under both the CPA and the DPDP Act, highlighting the severe compliance challenge:

	; Dark Pattern;	**; CPA2019(Unfair Trade Practice)**	**DPDPAct2023 (Data Privacy Violation)**
; 1.	; Forced Action;	Coercing a consumer into an unintended action (e.g., sharing contacts) to complete a transaction, thereby restricting consumer choice.;	Violation of Purpose Limitation and Data Minimisation principles. Invalidates consent as it is conditional on receiving the service.;
; 2.	; Basket Sneaking;	Automatically adding items(e.g., charity contribution ,insurance) to a cart without explicit consent, leading to unexpected charges.;	Processing of payment data without "unconditional" consent. Violation of Fair Processing and the duty to ensure data is not

	; Dark Pattern;	; CPA2019(Unfair Trade Practice)	DPDPAct2023 (Data Privacy Violation)
			processed in a manner detrimental to the Data Principal.;
; 3.	; Confirm shaming;	Using guilt or shame to influence a purchase or data sharing decision, exploiting psychological vulnerabilities.;	Consent obtained is not "free" or "unconditional," rendering it invalid under Section 4 (1)(a). The practice is inherently unfair and non-transparent
; 4.	; Subscription Trap;	.; Making cancellation excessively difficult or requiring unnecessary data for a free trial, leading to involuntary financial loss	.; Violation of the Right to Erasure and Data Minimisation. The continued processing of data after the purpose is served is unlawful.;
; 5.	; Pre -tic ked Boxes;	Deceptive practice that leads to the purchase of unwanted goods or services ,or the sharing of unwanted data.;	Violation of the requirement for unambiguous and affirmative consent. The consent is passive and therefore invalid.

Table 1: Dark patterns that give rise to simultaneous liability under the Consumer Protection Act, 2019 and the Digital Personal Data Protection Act, 2023.

The CCPA has already demonstrated its willingness to act, as seen in the enforcement actions against major e-commerce and travel platforms for 'Basket Sneaking'[5]. While these actions were taken under the CPA, the underlying harm— the non-consensual use of consumer data and payment information— is fundamentally a data privacy issue. The DPDP Act, with its much higher financial penalties (up to ₹250 crore for severe violations) [6], significantly raises the stakes for businesses that fail to align their commercial practices with data protection principles. The combined regulatory threat necessitates a fundamental shift in business design philosophy from manipulative engagement to ethical data stewardship.

IV. Jurisdictional Overlap and Regulatory Challenges

While the dual framework offers enhanced protection, it also introduces complexities regarding jurisdiction and enforcement, particularly concerning the respective roles of the Data Protection Board (DPB) and the Consumer Dispute Redressal Commissions (CDRCs).

[5] AZB & Partners, *Regulatory Crackdown on Dark Patterns: CCPA's Enforcement Actions and Emerging Compliance Landscape in Indian E-Commerce*, available at <https://www.azbpartners.com/bank/regulatory-crackdown-on-dark-patterns-ccpas-enforcement-actions-and-emerging-compliance-landscape-in-indian-e-commerce/> accessed 22 August 2026.

[6] The Digital Personal Data Protection Act, 2023, s. 33 read with the Schedule (maximum penalty of ₹250 crore for failure to take reasonable security safeguards).

A. Dual Grievance Redressal Mechanisms

The DPDP Act mandates that a Data Principal must first approach the Data Fiduciary's designated officer to redress a grievance. If unsatisfied, the Data Principal can then escalate the matter to the DPB. The DPB's mandate is strictly focused on enforcing the provisions of the DPDP Act, including investigating data breaches and imposing penalties for non-compliance. The DPB is an expert body designed to handle the technical and legal complexities of data protection.

In parallel, the CPA provides a three-tier system of CDRCs (District, State, and National) for consumers to seek redressal for unfair trade practices, defective goods, or deficient services. Furthermore, the CCPA can initiate investigations and issue directions against UTPs. The CCPA and the CDRCs are primarily concerned with the commercial harm and unfairness caused to the consumer.

This creates a scenario of dual grievance forums where a single incident— for example, a data breach leading to financial loss or a dark pattern leading to unauthorized data sharing— could potentially be litigated in two separate forums:

- Before the DPB: For violation of the Data Fiduciary's duty to protect personal data (Section 8(4)) or failure to obtain valid consent (Section 4). The remedy here is primarily punitive (penalties) and corrective (directions to mitigate).
- Before the CDRCs: For deficiency in service or an unfair trade practice that caused financial or mental distress to the consumer. The remedy here is primarily compensatory (damages) and corrective (refunds, discontinuation of UTP).

This jurisdictional overlap can lead to forum shopping by consumers seeking the most favorable outcome, or, conversely, double jeopardy for businesses facing parallel proceedings for the same underlying set of facts. The lack of explicit, coordinated guidance between the CCPA and the DPB, a feature present in mature jurisdictions like the UK (where the Information Commissioner's Office (ICO) and the Competition and Markets Authority (CMA) issue joint guidance) [7], creates regulatory uncertainty in India. The risk is that the two bodies may issue conflicting findings or remedies, undermining the coherence of the regulatory framework. For instance, a consumer may claim a dark pattern is an UTP before the CCPA, while simultaneously claiming the resulting data processing is a violation of the DPDP Act before the

[7] Competition and Markets Authority and Information Commissioner's Office, *Competition and Data Protection in Digital Markets: A Joint Statement between the CMA and the ICO* (19 May 2021), available at <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf> accessed 22 August 2026.

 [ISSN 2581-5369]

DPB. Without a clear mechanism for cross-referencing and deference, this situation poses a significant challenge to judicial efficiency and regulatory clarity.

B. Conflict of Rights: Erasure versus Retention

A significant point of potential conflict lies in the tension between the Data Principal's Right to Erasure under the DPDP Act and the mandatory Record Retention requirements under the CPA and other e-commerce rules.

The DPDP Act stipulates that a Data Fiduciary must erase personal data once the purpose for which it was collected is served, or upon the withdrawal of consent. However, e-commerce platforms and service providers are often legally required to retain transaction records for a minimum period to comply with:

• Tax and Accounting Laws: For audit and compliance purposes.

• Consumer Dispute Resolution: To process refunds, chargebacks, or defend against consumer complaints filed under the CPA.

If a consumer exercises their right to erasure immediately after a transaction, the Data Fiduciary faces a legal dilemma: complying with the DPDP Act could lead to non-compliance with the CPA's requirements for record-keeping necessary for dispute resolution. The resolution of this conflict will likely require the DPB to clarify that legal obligations under other statutes, such as the CPA, constitute a "legitimate use" or "purpose" for which data can be retained, overriding the immediate right to erasure until the statutory retention period expires. The DPDP Act provides for certain "legitimate uses" where consent is not required, and it is imperative that the final rules clarify that compliance with other statutory obligations, particularly those protecting consumer rights and financial integrity, falls under this exception. This clarification is crucial for maintaining the integrity of the consumer redressal system.

V. Global Context and Future Directions

The challenges faced by India in harmonizing data privacy and consumer protection are not unique. A brief comparison with global models highlights the path forward for India's regulatory framework.

India's current model, with the DPDP Act and the CPA, most closely resembles the EU model in its dual legislative approach, but it currently lacks the formal, coordinated enforcement mechanisms seen in the EU and UK. The US model, where the FTC acts as a single, powerful regulator for both privacy and consumer protection, offers a different, more centralized

 [ISSN 2581-5369]

approach. India's decision to create two separate bodies— the DPB and the CCPA— necessitates a strong focus on inter-agency cooperation.

Jurisdiction;	Primary Privacy Law;	Primary Consumer Law;	Mechanism for Intersection;
European Union;	Genera l Data Protection Regulation (GDPR);	Unfair Commercial Practices Directive (UCPD);	Integrated enforcement; data privacy violations can be UCPs. European Data Protection Board (EDPB) and national consumer bodies coordinate.;
United States;	State-level laws (e.g., CCPA/CPRA);	Federal Trade Commission Act (FTC Act);	FTC enforces both privacy and consumer protection under Section 5 ("unfair or deceptive acts or practices").;
United Kingdom;	UK GDPR;	Consumer Protection from Unfair Trading Regulations 2008;	Joint guidance and cooperation between the Information Commissioner' s Office (ICO)and the Competition and Markets Authority (CMA).;

Table 2: Comparative approaches to data protection and consumer protection enforcement.

VI. Recommendations for an Integrated Framework

To maximize the protective synergy of the DPDP Act and the CPA, and to reduce regulatory uncertainty, the following steps are recommended:

13. Coordinated Regulatory Guidance and Memorandum of Understanding (MoU): The DPB and the CCPA must establish a formal mechanism for cooperation, ideally through a Memorandum of Understanding (MoU). This MoU should outline clear protocols for information sharing, joint investigations, and, most importantly, a framework for determining which body takes the lead in cases of overlapping jurisdiction. Joint advisories on issues like dark patterns, data retention, and the handling of dual-nature grievances are essential to provide clarity to businesses and ensure consistent application of the law.

14. Integrated Compliance Systems and Privacy by Design: Businesses must move away from siloed compliance teams. Privacy policies and consumer terms of service should be drafted together to ensure consistency. More importantly, the principle of Privacy by Design must be integrated with Ethical Design principles. This means that digital interfaces should be designed from the outset to promote consumer autonomy and data minimization, rather than manipulation. A unified grievance redressal system, where a single officer is trained to handle

 [ISSN 2581-5369]

both privacy and consumer complaints, should be implemented to streamline the consumer experience.

15. Legislative Clarification on Conflicts: The rules and regulations under the DPDP Act must explicitly address the conflict between the Right to Erasure and statutory record retention requirements under the CPA, providing a clear hierarchy of obligations. The rules should confirm that data retention required for compliance with the CPA (e.g., for processing refunds or handling disputes) constitutes a "legitimate use" under the DPDP Act, thereby allowing the Data Fiduciary to temporarily override the right to erasure for that specific, limited purpose.

16. Focus on Digital Autonomy and Behavioral Economics: Future regulatory efforts should continue to focus on the concept of digital autonomy, ensuring that the consumer's right to make free and informed choices— both commercial and informational— is protected from all forms of manipulation. The CCPA's focus on dark patterns is a commendable step in applying behavioral economics to consumer protection, and this approach should be further extended to other areas where data-driven personalization can lead to consumer detriment, such as price discrimination based on personal data.

VII. Conclusion

The Digital Personal Data Protection Act, 2023, and the Consumer Protection Act, 2019, together represent a significant leap forward in safeguarding the rights of the Indian digital consumer. The DPDP Act provides the fundamental right to informational privacy, while the CPA, through its robust framework against Unfair Trade Practices and the specific targeting of dark patterns, ensures that this right is not subverted by commercial manipulation.

The intersection of these two laws is a powerful one. It transforms the violation of data privacy — once a matter of technical compliance— into a matter of consumer fairness and commercial ethics. The use of dark patterns, which exploit the consumer's data and subvert their

autonomy, is now a high-risk activity, exposing businesses to the severe penalties of the DPDP Act and the enforcement actions of the CCPA.

While the framework is robust in principle, the challenge lies in its execution. The successful realization of this dual protection hinges on the ability of the Data

Protection Board and the Central Consumer Protection Authority to establish clear, coordinated enforcement mechanisms. By doing so, India can solidify its position as a leader in digital governance, ensuring that the growth of its digital economy is built on a foundation of trust, transparency, and respect for the fundamental rights and autonomy of the consumer.

 [ISSN 2581-5369]