

The Convergence of Deceptive Design and Vitiating Consent: A Doctrinal Conflict Between the CCPA Dark Patterns Guidelines and the DPDP Act, 2023

Asst. Prof. Chinmay Powar

Assistant Professor

D.E.S. Shri Navalmal Firodia Law College, Pune

Abstract

The trajectory of India's digital economy, accelerated by post-pandemic platformisation and a regulatory architecture still in its formative phase, has produced a peculiar regulatory pathology: user-interface design has migrated from a marketing variable into a juridical instrument capable of overriding statutory autonomy. This paper interrogates the doctrinal collision between two near-simultaneously enacted instruments—the Central Consumer Protection Authority's Guidelines for Prevention and Regulation of Dark Patterns, 2023, framed under the Consumer Protection Act, 2019, and Section 6 of the Digital Personal Data Protection Act, 2023. Where a platform deploys deceptive choice architecture to extract data, the act simultaneously constitutes an unfair trade practice and an ab initio vitiating of 'free, specific, informed, unconditional, and unambiguous' consent. The result is a regulatory blind spot, a latent double-jeopardy controversy under Article 20(2) of the Constitution, and a structural enforcement asymmetry that sophisticated tech conglomerates can arbitrage. Drawing on comparative insights from the EU Digital Services Act and the United States Federal Trade Commission's enforcement experience, this paper advocates a harmonised, 'Fairness-by-Design' framework anchored in mandatory interface audits and a formal coordination mechanism between the CCPA and the Data Protection Board of India.

Keywords: Dark patterns; vitiating of consent; DPDP Act, 2023; CCPA Guidelines, 2023; choice architecture; algorithmic coercion; Fairness-by-Design; double jeopardy; Article 20(2); Digital Services Act.

PART I

Introduction and the Cognitive Psychology of Growth Hacking

India's digital marketplace has, within the span of a single decade, transitioned from a frontier of unmet demand into a saturated theatre of behavioural competition. The transaction volume on the Unified Payments Interface alone now exceeds the combined retail payment systems of several G-20 economies (Reserve Bank of India, 2024), and the user base of platform-mediated commerce is projected to cross 900 million by 2027 (Powar, 2026). What is less frequently observed, however, is that this remarkable scale has been achieved not through traditional price competition but through a quieter and far more consequential contest over the cognitive bandwidth of the consumer. Platforms have learnt that the marginal user is no longer persuaded; she is engineered.

The migration from persuasive marketing to what may be described as choice-architecture coercion is the doctrinal pivot on which this paper turns. Persuasion, in its classical Aristotelian sense, presupposes a deliberating agent capable of weighing competing reasons (Cialdini, 2007). Choice architecture, by contrast, operates at the level of the pre-reflective: the placement of a button, the chromatic salience of a hyperlink, the silent toggling of a privacy default. Thaler and Sunstein famously theorised that such design choices could be deployed as benevolent 'nudges' to steer individuals towards welfare-enhancing outcomes (Thaler and Sunstein, 2008). Indian platform practice, regrettably, has inverted this premise. What now confronts the regulator is the malignant nudge—a deliberate, monetised inversion of libertarian paternalism in which the choice architect is no longer a benevolent planner but an interested commercial party (Sunstein, 2020; Luguri and Strahilevitz, 2021).

Dark patterns, accordingly, must not be reduced to the prosaic vocabulary of 'bad design' or 'poor user experience'. They are, in their juridical essence, the systematic exploitation of identifiable cognitive heuristics for the extraction of

consent, attention, or expenditure that the user, under conditions of informed deliberation, would not have surrendered. Loss aversion—the empirically robust finding that the disutility of losing a unit of value exceeds the utility of acquiring it (Kahneman and Tversky, 1979)—is weaponised through countdown timers, expiring carts, and confirm-shaming dialogues that frame opt-out as forfeiture. Default bias is operationalised through pre-ticked consent boxes that route the inattentive user into data-sharing arrangements she has never affirmatively endorsed (Sunstein, 2020). Scarcity cues—‘only two rooms left at this price’—co-opt the consumer's appraisal system and short-circuit comparative reasoning (Mathur et al., 2019).

The legal significance of this transition is that design no longer ornaments the transaction; it constitutes it. The interface is the contract. When a registration screen renders the ‘Accept All’ button in vivid emerald and consigns the ‘Manage Preferences’ option to greyscale six points smaller, the platform has not merely solicited consent—it has manufactured it. The autonomy that Section 6 of the Digital Personal Data Protection Act, 2023 demands and that Section 2(47) of the Consumer Protection Act, 2019 presupposes is, in such a moment, structurally unavailable to the user (Digital Personal Data Protection Act, 2023, s. 6; Consumer Protection Act, 2019, s. 2(47)). Consent, in the language of the older contract jurisprudence, has been obtained by undue influence dressed in the silk of design (Mulla, 2018).

This introductory framing yields the central proposition of the paper. The doctrinal question is not whether dark patterns are wrongful—both the Central Consumer Protection Authority and Parliament have answered that affirmatively—but whether the wrong is a consumer wrong, a data-protection wrong, or, as this paper contends, a single wrong refracted through two statutory prisms (Central Consumer Protection Authority, 2023; Digital Personal Data Protection Act, 2023). The answer will determine the locus of remedy, the calibration of penalty, and, ultimately, whether India's regulatory response coheres into doctrine or fragments into turf.

Footnotes

[1] Reserve Bank of India, Payment System Indicators (Monthly Bulletin, March 2024). UPI monthly transaction volumes have consistently exceeded INR 18 lakh crore since the fourth quarter of FY 2023-24.

[2] R. H. Thaler and C. R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* (Yale University Press, 2008) 3-6. The authors define ‘choice architecture’ as any feature that organises the context in which people make decisions.

[3] Cass R. Sunstein, ‘Sludge Audits’ (2020) 36(2) *Journal of Risk and Uncertainty* 1-21. Sunstein himself has acknowledged the asymmetric weaponisation of nudge theory by commercial actors, terming the inverse phenomenon ‘sludge’.

[4] J. Luguri and L. J. Strahilevitz, ‘Shining a Light on Dark Patterns’ (2021) 13 *Journal of Legal Analysis* 43, 67-71, presenting experimental evidence that aggressive dark patterns increase opt-in rates fourfold relative to neutral interfaces.

[5] D. Kahneman and A. Tversky, ‘Prospect Theory: An Analysis of Decision under Risk’ (1979) 47(2) *Econometrica* 263-291. Loss aversion is the foundational behavioural finding repurposed by interface designers for retention engineering.

[6] A. Mathur et al., ‘Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites’ (2019) 3 *Proceedings of the ACM on Human-Computer Interaction (CSCW)* Article 81, 1-32.

[7] Consumer Protection Act 2019 (No. 35 of 2019), s. 2(47), defining ‘unfair trade practice’ in inclusive and expansive terms.

[8] Digital Personal Data Protection Act 2023 (No. 22 of 2023), s. 6(1), requiring that consent be ‘free, specific, informed, unconditional and unambiguous with a clear affirmative action’.

[9] Sir Dinshaw Fardunji Mulla, *The Indian Contract and Specific Relief Acts* (15th edn, LexisNexis, 2018) commentary on ss. 13-16, which collectively articulate the consensual core of Indian contract law and the doctrines that vitiate it—coercion, undue influence, fraud, misrepresentation, and mistake.

[10] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023 (Notification No. CCPA/Dark Patterns/2023, dated 30 November 2023), preamble and Annexure, enumerating thirteen specified dark patterns.

PART II

The Indian Regulatory Landscape: A Dual-Statutory Analysis

Two instruments now occupy the doctrinal terrain on which dark patterns are to be evaluated. They emerged from different ministries, address different harms, and deploy different enforcement architectures, yet they converge upon the same transactional moment: the user's click. A close, section-by-section examination of each instrument is therefore the prerequisite to any serious analysis of the doctrinal conflict that the third part of this paper develops.

A. The CCPA Guidelines for Prevention and Regulation of Dark Patterns, 2023

The Central Consumer Protection Authority, constituted under Section 10 of the Consumer Protection Act, 2019, issued the Guidelines for Prevention and Regulation of Dark Patterns on 30 November 2023 in exercise of its powers under Sections 18(2)(l) and 18(2)(zg) of the parent statute (Central Consumer Protection Authority, 2023). These Guidelines are not soft law in the colloquial sense; they derive binding force from the parent enactment and operate by deeming the enumerated practices to constitute unfair trade practices within the meaning of Section 2(47).

The Guidelines define a 'dark pattern' as any practice or deceptive design pattern using user interface or user experience interactions on any platform that is designed to mislead or trick users to do something they originally did not intend or want to do, by subverting or impairing the consumer autonomy, decision-making or choice (Central Consumer Protection Authority, 2023, cl. 2(e)). Thirteen specified practices populate the Annexure. 'Basket sneaking' captures the surreptitious addition of items, donations, or insurance to the consumer's cart at the point of checkout, a practice that converts an act of purchase into an act of imposed subscription. 'Confirm-shaming' weaponises affect: the consumer who declines a newsletter is required to click 'No, I prefer to remain uninformed', a design that exploits the social cost of self-deprecation. 'Forced action' conditions access to a service on the user's submission of unrelated consents, marketing permissions, or biometric data. 'Interface interference', 'bait and switch', 'drip pricing', 'disguised advertisement', 'nagging', 'trick wording', 'SaaS billing', and 'rogue malware' each receive analogous treatment in the Annexure.

The juridical mechanism is elegant in its parsimony. Section 2(47) of the parent Act defines 'unfair trade practice' inclusively, capturing any practice that, for the purpose of promoting the sale, use, or supply of goods or services, adopts any unfair method or unfair or deceptive practice (Consumer Protection Act, 2019, s. 2(47)). The Guidelines, by deeming the enumerated dark patterns to fall within this provision, render them actionable before the District, State, and National Consumer Disputes Redressal Commissions, and enforceable by the CCPA itself under Section 21, with penalties extending under Sections 88 and 89 to imprisonment up to two years and fines up to ten lakh rupees for repeat offenders (Consumer Protection Act, 2019, ss. 21, 88, 89).

The conceptual frame in which the CCPA operates is the protection of consumer autonomy understood transactionally. The harm contemplated is the distortion of a purchase decision—whether to buy, what to buy, how much to pay. The remedy is calibrated accordingly: deterrence through penalty and disgorgement, restitution through refund, and prevention through cease-and-desist directions (Powar, 2026). The user, in this frame, is a consumer; the wrong is a market wrong; the autonomy protected is economic.

B. Section 6 of the Digital Personal Data Protection Act, 2023

Section 6 of the DPDP Act, 2023 occupies the same UI-mediated transactional moment from a wholly different doctrinal angle. Its provenance lies in the constitutional right to informational privacy recognised by the Supreme Court in *K. S. Puttaswamy v. Union of India* (2017), and its operative logic is the protection of personality rather than the protection of pocket (*Justice K. S. Puttaswamy (Retd.) v. Union of India*, 2017). Section 6(1) requires that the consent given by the Data Principal be 'free, specific, informed, unconditional and unambiguous with a clear affirmative action', and that it signify an agreement to the processing of personal data for the specified purpose and be limited to such personal data as is necessary for such purpose (Digital Personal Data Protection Act, 2023, s. 6(1)).

Each adjective in that quintuple formulation carries doctrinal weight. ‘Free’ imports the contractual jurisprudence of Section 14 of the Indian Contract Act, 1872, and the cognate doctrines of coercion, undue influence, fraud, and misrepresentation. ‘Specific’ imports the EU-derived principle of purpose limitation, prohibiting omnibus consents that would license downstream processing for unenumerated purposes (Article 29 Working Party, 2018). ‘Informed’ imports Section 5 of the DPDP Act, which obliges the Data Fiduciary to provide a notice describing the personal data and the purpose of processing in clear and plain language (Digital Personal Data Protection Act, 2023, s. 5). ‘Unconditional’ prohibits the bundling of consent to processing with consent to terms of service, a practice that the EU Court of Justice condemned in *Bundeskartellamt v. Meta Platforms* (2023). ‘Unambiguous’, finally, requires affirmative conduct: silence, inaction, or pre-ticked boxes cannot constitute consent (Article 29 Working Party, 2018).

The architecture of Section 6 is reinforced by Section 7, which exhaustively enumerates the limited grounds of ‘legitimate uses’ on which a Data Fiduciary may process personal data in the absence of consent, and by Sections 8 and 9, which impose obligations of accuracy, security, and breach notification on the Data Fiduciary (Digital Personal Data Protection Act, 2023, ss. 7-9). The enforcement architecture is housed in the Data Protection Board of India, constituted under Chapter V, with adjudicatory powers under Section 33 and penalty-imposing powers under Section 33 read with the Schedule. The Schedule prescribes financial penalties extending up to two hundred and fifty crore rupees for failure to take reasonable security safeguards, and graduated penalties for other contraventions including the obtaining of consent in a manner non-compliant with Section 6 (Digital Personal Data Protection Act, 2023, Schedule).

The conceptual frame, then, is fundamentally distinct. Where the CCPA conceives the user as a consumer and the wrong as market distortion, the DPDP Act conceives the user as a Data Principal and the wrong as the unauthorised processing of an informationally embodied self. The autonomy protected is dignitary, not transactional; the remedy is calibrated to deter the data-extractive enterprise rather than to refund the deceived purchaser (Bhandari and Sane, 2023). It is this asymmetry of conceptual frame, despite the identity of the transactional moment, that generates the doctrinal conflict to which Part III now turns.

Footnotes

[11] Consumer Protection Act 2019 (No. 35 of 2019), s. 10, constituting the Central Consumer Protection Authority, and ss. 18(2)(l) and 18(2)(zg), conferring rule-making and guideline-issuing powers.

[12] Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns 2023, cl. 2(e). The definition is deliberately expansive and technology-neutral so as to capture as-yet-unidentified design practices.

[13] Ibid, Annexure, paras 1-13, enumerating false urgency, basket sneaking, confirm-shaming, forced action, subscription trap, interface interference, bait and switch, drip pricing, disguised advertisement, nagging, trick wording, SaaS billing, and rogue malware.

[14] Consumer Protection Act 2019, s. 88 (penalty for non-compliance with directions of the Central Authority): imprisonment up to six months, or fine up to twenty lakh rupees, or both; s. 89 (punishment for false or misleading advertisement): up to two years imprisonment and ten lakh rupees fine for first offence.

[15] Justice K. S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, recognising informational privacy as a facet of the fundamental right to privacy under Article 21 of the Constitution.

[16] Digital Personal Data Protection Act 2023, s. 6(1).

[17] Indian Contract Act 1872, ss. 13-19A, articulating the requirement of ‘free consent’ and the doctrines that vitiate it.

[18] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679 (WP259 rev.01, 10 April 2018), 5-7, articulating the ‘four elements’ of valid consent under the GDPR, on which the DPDP Act draws substantially.

[19] Case C-252/21 *Meta Platforms Inc. v. Bundeskartellamt* [2023] ECLI:EU:C:2023:537, [150]-[154], holding that consent bundled with service access cannot be regarded as freely given where a dominant undertaking is involved.

[20] Digital Personal Data Protection Act 2023, Schedule. The maximum financial penalty is INR 250 crore for breach of reasonable security safeguards; INR 200 crore for failure to fulfil consent-related obligations; and INR 150 crore for breaches concerning children's data.

[21] V. Bhandari and R. Sane, 'A Critique of the DPDP Act, 2023' (NIPFP Working Paper, October 2023) 14-17, observing the asymmetry between consent-policing duties and the absence of an explicit 'fairness' principle in the Act.

PART III

The Doctrinal Conflict: Vitiating Consent vs. Consumer Choice

The doctrinal collision proceeds from a singular fact: in the architecture of the modern platform, the act that triggers consumer detriment and the act that transmits data consent are not merely related; they are coterminous. The click on 'Accept All' is, in one and the same instant, a transactional acceptance regulated by the Consumer Protection Act and a consent transmission regulated by the DPDP Act. When that click has been engineered by a deceptive interface, the Indian legal system must answer a question for which it has no settled grammar: what is the juridical status of a single act that two statutes simultaneously, and by different criteria, condemn?

A. Privacy Zuckering and the Phenomenology of Engineered Consent

The term 'Privacy Zuckering', popularised in the international human-computer-interaction literature and named for the architectural choices of the Meta family of products, denotes the deliberate construction of an interface that obscures, attenuates, or punishes the exercise of privacy-protective choices while accelerating and rewarding the surrender of personal data (Brignull, 2010; Mathur et al., 2019). Its mechanisms are by now well-documented. The opt-in to data sharing is rendered in a saturated primary colour, occupies the centre of the modal, and requires a single tap. The opt-out is achromatic, peripheral, two-levels-deep within a settings menu, and is followed by a confirm-shaming interstitial. The cumulative effect, as Luguri and Strahilevitz's randomised experiments establish, is to quadruple opt-in rates relative to neutral baselines (Luguri and Strahilevitz, 2021).

The phenomenology of this engineered consent is what places it beyond the consoling fiction of 'notice and choice'. The user has, in a strict operational sense, clicked. She has, in a formal sense, agreed. Yet the deliberative process that the consent form purports to memorialise has been structurally pre-empted. Section 14 of the Indian Contract Act, 1872, defines consent as 'free' when it is not caused by coercion, undue influence, fraud, misrepresentation, or mistake (Indian Contract Act, 1872, s. 14). The doctrines of undue influence and misrepresentation, properly understood, are capable of capturing the phenomenology of dark patterns. The platform stands in a position to dominate the user's will—not through familial or fiduciary authority, as the older case law contemplated, but through the asymmetric informational and architectural power that the closed interface confers (Mulla, 2018; Powar, 2026).

B. The Doctrine of Ab Initio Vitiating

If the foregoing analysis is accepted, the consequence under the DPDP Act is immediate and structural. Section 6(10) of the Act provides that where consent has not been obtained in conformity with the requirements of Section 6, the processing carried out on the basis of such consent is unlawful (Digital Personal Data Protection Act, 2023, s. 6(10)). The consent is, in the classical formulation, void ab initio. There is no severance, no curing, no good-faith defence. The platform that has secured consent through Privacy Zuckering is, from the moment of the engineered click, processing data without lawful basis and is exposed to the full penalty regime under the Schedule.

The analytical force of this conclusion lies in its simultaneity with the parallel conclusion under the Consumer Protection Act. The same engineered click is, concurrently, the consummation of an unfair trade practice under Section 2(47) read with the CCPA Guidelines. Two statutes, two regulators, one act. The doctrinal question is not whether to apply one or the other, but whether the Indian legal system possesses the analytical equipment to apply both coherently.

C. The Paradox of Apparent Choice

Consider the following constructed but representative scenario. A user installs an Indian fintech application. The onboarding screen presents a single, brightly coloured button reading 'Continue'. Adjacent to that button, in light grey

six-point type, appears the text ‘By continuing, you accept our Privacy Policy and consent to the processing of your contacts, location, SMS metadata, and device identifiers for marketing, credit profiling, and partner offers’. The user taps ‘Continue’. Has she consented?

The CCPA's analytical apparatus answers in the negative on the ground that the interface constitutes ‘trick wording’ and ‘interface interference’ within the Guidelines’ Annexure, and that the resulting transactional outcome constitutes an unfair trade practice (Central Consumer Protection Authority, 2023). The DPDP Act's analytical apparatus also answers in the negative, on the cognate but distinct ground that the consent is neither ‘informed’ (the notice is buried), nor ‘specific’ (the purposes are aggregated), nor ‘unconditional’ (consent is bundled with access), nor produced through a ‘clear affirmative action’ (the tap is on ‘Continue’, not on any element labelled as consent) (Digital Personal Data Protection Act, 2023, s. 6).

Two different statutory regimes, applying two different conceptual frames, reach the same descriptive conclusion through two different doctrinal routes. This is not, in itself, a defect; convergent regulation may be the rational response to a multifaceted wrong. The defect emerges in the next analytical step. The consumer wrong is calibrated to the transaction—to the unfair extraction of money or the unfair imposition of an unwanted product. The data wrong is calibrated to the personality—to the unauthorised processing of an informationally embodied self. The remedies, the standards of proof, and the procedural architectures diverge accordingly. A user who has been Zuckered is not merely a consumer who has been deceived; she has, at a deeper analytical level, had her informational personality conscripted into a commercial enterprise (Cohen, 2019). The two statutes capture different layers of a single harm, and the Indian regulator must decide whether they will be applied cumulatively, alternatively, or harmoniously.

D. Algorithmic Coercion and the Reformulation of Free Consent

The deeper jurisprudential reformulation that this analysis invites is the recognition of algorithmic coercion as a *sui generis* vitiating factor. Classical Indian contract law contemplated coercion in terms of physical or quasi-physical threat (Indian Contract Act, 1872, s. 15). Undue influence contemplated the abuse of relational power (Indian Contract Act, 1872, s. 16). Neither doctrine cleanly captures the asymmetric architectural power that the platform deploys against the atomised user. Yet the functional equivalence is striking. The user faces a closed interface designed by parties she cannot identify, optimised against metrics she cannot observe, deploying behavioural insights she cannot articulate, and from which exit is either impossible (the platform is a monopolist or near-monopolist) or prohibitively costly (network effects have foreclosed alternatives). To describe the resulting click as ‘free’ is to ignore the architecture that produced it (Hartzog, 2018).

Algorithmic coercion, properly theorised, would extend the doctrinal reach of Section 6 of the DPDP Act and Section 2(47) of the Consumer Protection Act into the territory that traditional contract doctrine has not adequately mapped. It would require courts and regulators to evaluate consent not by reference to the formal moment of the click but by reference to the architectural conditions under which the click occurred. The interface, in this analytic frame, is itself the object of legal scrutiny—a position that the Federal Trade Commission has adopted in its recent enforcement against deceptive subscription models (Federal Trade Commission, 2023) and that the EU Court of Justice has signalled in *Bundeskartellamt v. Meta* (Case C-252/21, 2023).

Footnotes

[22] H. Brignull, ‘Dark Patterns: User Interfaces Designed to Trick People’ (2010), the originating taxonomy from which subsequent regulatory categories, including those of the CCPA Guidelines, are descended.

[23] Mathur et al. (n 6), 14-19, demonstrating empirically that Privacy Zuckering patterns appear on over 11 per cent of large-scale e-commerce platforms surveyed.

[24] Luguri and Strahilevitz (n 4), 67-71.

[25] Indian Contract Act 1872, s. 14: ‘Consent is said to be free when it is not caused by—(1) coercion, as defined in section 15, or (2) undue influence, as defined in section 16, or (3) fraud, as defined in section 17, or (4) misrepresentation, as defined in section 18, or (5) mistake, subject to the provisions of sections 20, 21 and 22.’

[26] Digital Personal Data Protection Act 2023, s. 6(10), providing that consent given in breach of the Act ‘shall be invalid to the extent of such breach’.

[27] Indian Contract Act 1872, s. 15 (coercion); s. 16 (undue influence). For a doctrinal reading of these provisions in the contemporary context, see Pollock and Mulla, *The Indian Contract and Specific Relief Acts* (15th edn, 2018) Vol I, ch. 4.

[28] J. E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press, 2019) 47-58, theorising the platform's extraction of informationally embodied selves as a constitutive feature of contemporary capitalism.

[29] W. Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Harvard University Press, 2018) 21-44, articulating the case for treating design as the proper object of privacy regulation.

[30] Federal Trade Commission, Negative Option Rule, 88 Fed. Reg. 24,716 (proposed 24 April 2023); see also *FTC v. Amazon.com Inc., Complaint*, Case No. 2:23-cv-00932 (W.D. Wash., 21 June 2023), alleging deceptive Prime enrolment and cancellation interfaces.

PART IV

The Enforcement Deficit and Jurisdictional Overlap

Doctrinal convergence on the wrongfulness of dark patterns does not translate, in the Indian regulatory landscape, into convergence at the level of enforcement. The Central Consumer Protection Authority and the Data Protection Board of India operate on distinct enabling statutes, report to different ministries, command different remedial inventories, and dispose of penalties separated by orders of magnitude. A platform whose interface contravenes both regimes thus confronts not one enforcement risk but two, and a regulator confronts not a clear allocation of jurisdiction but a contested one. The result is at once an enforcement deficit and a constitutional puzzle.

A. The Penalty Asymmetry

The first and most arresting feature of the dual regime is the asymmetry of penalty. The Consumer Protection Act, in its current configuration, exposes a contravening platform to a maximum financial penalty of ten lakh rupees for a first offence under Section 89, with an upper ceiling of fifty lakh rupees for repeat misleading advertisement (Consumer Protection Act, 2019, ss. 88-89). The DPDP Act, by contrast, prescribes financial penalties extending to two hundred and fifty crore rupees for failures in respect of reasonable security safeguards, and two hundred crore rupees for breaches of consent-related obligations under Sections 6 and 7 (Digital Personal Data Protection Act, 2023, Schedule). The DPDP Act's maximum penalty is, accordingly, approximately twenty-five-thousand times the maximum penalty under the Consumer Protection Act for what may, in the case of dark patterns, be the identical underlying conduct.

The disparity is not merely numerical; it is structural. A penalty of ten lakh rupees is, for a platform with annual revenues in the tens of thousands of crores, operationally indistinguishable from a regulatory rounding error. A penalty of two hundred and fifty crore rupees is, conversely, a material item on the income statement of even the largest fiduciaries. The deterrent calculus that each regulator can credibly deploy is therefore differential, and the platform's compliance investment will, predictably, be calibrated to the DPDP exposure rather than the CCPA exposure (Powar, 2026). The CCPA's normative authority over the interface is, in operational terms, parasitic upon the DPBI's penalty regime.

B. The Jurisdictional Loophole

A platform that has engineered a Privacy Zuckering interface confronts two regulators, each of whom may legitimately claim jurisdiction. The CCPA may initiate inquiry under Section 19 of the Consumer Protection Act on the ground that the practice falls within the deeming language of the 2023 Guidelines. The DPBI may initiate inquiry under Section 33 of the DPDP Act on the ground that consent so obtained is invalid under Section 6(10). Neither statute contains a non-obstante clause that subordinates the other; neither statute contains a coordination provision that compels the two regulators to confer (Bhandari and Sane, 2023).

The structural consequence is two-fold. The first is the prospect of forum-shopping by the complainant, who, in the absence of allocation rules, may select the regulator likely to deliver the more expeditious or generous remedy. The second, and more concerning, is the prospect of regulatory free-riding by the platform, which may exploit the absence

of coordinated investigation to settle with one regulator on terms that the other regulator might not have accepted. In the experience of similarly bifurcated regulatory regimes in other jurisdictions, such fragmentation produces a downward spiral of enforcement (Bamberger and Mulligan, 2015). The Indian dual regime, as currently configured, is structurally vulnerable to precisely this dynamic.

C. Article 20(2) and the Double Jeopardy Question

The constitutional question that the dual regime raises with particular acuity is whether successive or simultaneous proceedings before the CCPA and the DPBI for the same interface design would offend Article 20(2) of the Constitution, which prohibits the prosecution and punishment of any person for the same offence more than once (Constitution of India, 1950, art. 20(2)). The doctrinal answer, on current authority, is in the negative—but only in the negative in a qualified sense that itself merits examination.

Article 20(2) is, by settled Supreme Court jurisprudence, confined to criminal prosecutions in the strict sense and is inapplicable to civil or administrative penalties (Maqbool Hussain v. State of Bombay, 1953; Thomas Dana v. State of Punjab, 1959). The penalties imposed by the CCPA under Section 88 of the Consumer Protection Act are characterised in part as criminal and in part as civil; the penalties imposed by the DPBI under the Schedule to the DPDP Act are exclusively civil. To the extent that both proceedings are civil, Article 20(2) does not apply. To the extent that the CCPA proceeding is criminal under Section 89, the argument that the DPBI proceeding constitutes a second prosecution ‘for the same offence’ founders on the doctrinal distinctness of the two offences: the offence under Section 89 is the false or misleading advertisement; the offence under the DPDP Schedule is the failure of consent-related obligation.

Yet to leave the analysis at this formalistic juncture is to misread the gravamen of the constitutional concern. The doctrine of issue estoppel, the common-law principle of *nemo debet bis vexari pro una et eadem causa*, and the broader administrative-law principle of proportionality each suggest that successive regulatory proceedings on the same factual substratum, even where Article 20(2) is not formally triggered, ought to be conducted with regard to the cumulative burden imposed on the regulated entity (V.K. Aggarwal v. Union of India, 1992). The absence of a statutory mechanism by which the CCPA and the DPBI must share evidence, coordinate timelines, and avoid cumulative penalty therefore creates not a constitutional violation in the technical sense but a constitutional infirmity in the structural sense (Powar, 2026). The platform, as the formally regulated entity, becomes the bearer of regulatory fragmentation costs that the State could, by modest legislative intervention, internalise.

D. The Asymmetric Capacity Problem

A final, less remarked-upon dimension of the enforcement deficit lies in the asymmetric institutional capacity of the two regulators. The CCPA, constituted in 2020 and operating from a modest secretariat in New Delhi, has, on publicly available data, fewer than fifty officers across all functions, including investigation, adjudication, and rule-making (Department of Consumer Affairs, 2024). The DPBI, although nominally constituted by the DPDP Act, has not at the date of writing been operationalised at full strength, and the appointment of its chairperson and members remains subject to executive notification. Each regulator, in its current incarnation, lacks the in-house technical capacity to conduct the kind of forensic interface audit that the doctrinal analysis of dark patterns actually requires. The forensic question—what did the user see, in what sequence, on what device, with what default settings?—is irreducibly empirical and technically demanding (Mathur et al., 2019). Neither regulator is presently equipped to answer it at scale.

Footnotes

[31] Consumer Protection Act 2019, ss. 88 and 89 (n 14).

[32] Digital Personal Data Protection Act 2023, Schedule (n 20).

[33] Bhandari and Sane (n 21), 18, noting the absence of any cross-statutory coordination provision.

[34] K. A. Bamberger and D. K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (MIT Press, 2015) 199-218, describing the dynamics of fragmented enforcement.

[35] Constitution of India 1950, art. 20(2): ‘No person shall be prosecuted and punished for the same offence more than once.’

[36] *Maqbool Hussain v. State of Bombay* AIR 1953 SC 325, [9]-[12], holding that departmental proceedings under the Sea Customs Act did not constitute ‘prosecution’ for the purposes of Article 20(2).

[37] *Thomas Dana v. State of Punjab* AIR 1959 SC 375, [27]-[33], reaffirming the criminal-prosecution-only construction of Article 20(2).

[38] *V.K. Aggarwal v. Union of India* (1992) 4 SCC 419, [14], invoking *nemo debet bis vexari* principles in the context of departmental and criminal proceedings on overlapping factual substrata.

[39] Department of Consumer Affairs, Annual Report 2023-24 (Ministry of Consumer Affairs, Food and Public Distribution, Government of India, 2024) 47-52, describing the sanctioned and filled strength of the Central Consumer Protection Authority.

[40] Mathur et al. (n 6), demonstrating the technical complexity of large-scale interface auditing and the methodological infrastructure such auditing requires.

PART V

Global Comparative Perspectives

The Indian regulator does not legislate on a blank slate. Two mature foreign jurisdictions—the European Union and the United States—have, in the preceding half-decade, developed substantial doctrinal and enforcement experience with the regulation of deceptive interface design. The comparative analysis that follows is offered not in the colonial register of borrowed wisdom but in the pragmatic register of accumulated empirical evidence. Each jurisdiction has, in its own configuration, confronted the same underlying conflict between consumer-protection and data-protection regimes; each has produced doctrinal innovations from which the Indian framework may, with appropriate adaptation, profitably draw.

A. The European Union: Digital Services Act and the GDPR Architecture

The European Union's Digital Services Act, 2022 (Regulation 2022/2065) represents the most ambitious legislative codification to date of the prohibition of deceptive interface design. Article 25 imposes a direct and comprehensive ban on dark patterns in the user interfaces of online platforms, providing that providers of online platforms ‘shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions’ (Digital Services Act, 2022, art. 25(1)). Article 31 supplements this prohibition with a positive obligation to design ‘online interfaces of online marketplaces’ such that traders can comply with their pre-contractual information obligations, thereby converting design from an unregulated commercial variable into a regulated compliance instrument (Digital Services Act, 2022, art. 31).

The doctrinal innovation of Article 25 lies in its express acknowledgement of the overlap with data-protection law. Article 25(2) provides that the prohibition applies without prejudice to Regulation 2016/679, the General Data Protection Regulation, and to Directive 2005/29 on unfair commercial practices (Digital Services Act, 2022, art. 25(2)). The European Data Protection Board has, in its Guidelines 03/2022 on Deceptive Design Patterns, articulated the corresponding GDPR framework, treating dark patterns as violations of the principles of fairness, transparency, and data minimisation under Article 5 of the GDPR (European Data Protection Board, 2022). The result is a coordinated dual regime in which the consumer-protection authority and the data-protection authority operate from a shared definitional vocabulary and proceed under harmonised interpretive guidelines—precisely the architecture that the Indian dual regime presently lacks.

The enforcement experience under this architecture, although still nascent, is instructive. In *Bundeskartellamt v. Meta Platforms* (Case C-252/21, 2023), the EU Court of Justice held that the bundling of data-processing consent with access to a dominant platform's services vitiates the freedom of consent under Article 7 of the GDPR (Case C-252/21, [150]-[154]). The reasoning is directly transposable to the Indian context: where a platform enjoys market dominance, the user's ‘choice’ to accept omnibus data-processing terms is not, in any meaningful sense, a choice (Powar, 2026).

The Bundeskartellamt judgment also demonstrates the productive coordination between competition, consumer-protection, and data-protection regulators that the EU architecture facilitates and the Indian architecture inhibits.

B. The United States: FTC Enforcement and the Roach Motel Doctrine

United States federal law lacks a unified data-protection statute analogous to the GDPR or the DPDP Act, but the Federal Trade Commission has, under Section 5 of the Federal Trade Commission Act, developed a robust enforcement jurisprudence around deceptive and unfair commercial practices that has expressly extended to dark patterns (Federal Trade Commission, 2022). The FTC's 2022 report, *Bringing Dark Patterns to Light*, articulates a doctrinal taxonomy of design practices deemed unfair or deceptive, with particular focus on subscription traps colloquially termed 'Roach Motels'—interfaces engineered to make enrolment frictionless and cancellation arduous (Federal Trade Commission, 2022).

The enforcement record is substantial. In *FTC v. Vonage* (2022), the Commission secured a \$100 million settlement in respect of cancellation interfaces that required telephone calls to non-functional numbers and the navigation of interactive voice-response systems engineered to dissuade rather than enable termination (Federal Trade Commission, 2022, *In re Vonage*). In *FTC v. Amazon.com* (2023), the Commission's complaint alleges that the Prime enrolment and cancellation interfaces were deliberately designed to obscure the cost of subscription and to multiply the steps required for cancellation, in violation of the Restore Online Shoppers' Confidence Act, 2010 (Federal Trade Commission, 2023, *FTC v. Amazon.com*).

Two features of the United States experience are of direct relevance to the Indian framework. The first is the doctrinal versatility of a single regulator vested with authority to address both deceptive design and the resulting harm to competition and consumer welfare. The FTC's structural unification of these functions avoids the inter-agency coordination problem that bedevils the Indian CCPA-DPBI architecture. The second is the FTC's empirical practice of conducting interface audits as a routine part of investigation, frequently in collaboration with academic researchers and external auditors (Federal Trade Commission, 2022). The Indian regulator's capacity gap, identified in Part IV, can be substantially addressed by adopting an analogous auditing methodology.

C. Comparative Insights for Indian Jurisprudence

Three insights crystallise from this comparative analysis. The first is definitional harmonisation: both the EU and the United States have converged on a shared operative definition of dark patterns that the consumer-protection and data-protection regulators apply in common, eliminating the doctrinal arbitrage that distinct definitions would otherwise enable. The Indian regulator should adopt a parallel definitional alignment between the CCPA Guidelines and any subordinate rules made under Section 40 of the DPDP Act (Powar, 2026).

The second is institutional coordination: the EU's coordinated dual regime, anchored in shared guidelines from the European Data Protection Board and the European Commission, and the United States' structural unification of regulatory authority each provide a model for resolving the jurisdictional overlap. India should formalise coordination between the CCPA and the DPBI through a statutory Memorandum of Understanding contemplated under Section 18(2)(j) of the Consumer Protection Act and any cognate rule-making power under the DPDP Act (Consumer Protection Act, 2019, s. 18(2)(j)).

The third is empirical methodology: both the EU and the United States have invested in the technical infrastructure required to audit interfaces at scale, whether through dedicated digital-enforcement units within the regulator or through collaboration with academic and civil-society researchers. The Indian regulator must invest in analogous capacity, and may consider the establishment of a joint technical secretariat between the CCPA and the DPBI as a cost-effective first step (Bhandari and Sane, 2023).

Footnotes

[41] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277/1, art. 25(1).

[42] Digital Services Act, art. 31, imposing online-interface design obligations on marketplaces; arts 25(2)-(3) preserving the operation of GDPR and the Unfair Commercial Practices Directive.

[43] European Data Protection Board, Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces (adopted 14 February 2023), 8-23.

[44] Case C-252/21 (n 19).

[45] Federal Trade Commission, Bringing Dark Patterns to Light (Staff Report, September 2022) 10-21.

[46] In re Vonage Holdings Corp., FTC Matter/File No. 2123076 (Stipulated Order, November 2022).

[47] FTC v. Amazon.com Inc., Case No. 2:23-cv-00932 (W.D. Wash., filed 21 June 2023); Restore Online Shoppers' Confidence Act, 15 U.S.C. §§ 8401-8405 (2010).

[48] Consumer Protection Act 2019, s. 18(2)(j), empowering the CCPA to advise the Central Government on consumer matters, a provision capable of accommodating formal inter-regulator coordination.

[49] Bhandari and Sane (n 21), 26-29, advocating institutional coordination as a necessary condition for credible enforcement of the DPDP Act.

PART VI

Policy Recommendations and Conclusion

The doctrinal and comparative analysis developed in the preceding parts converges on a single, structurally framed claim: India's regulatory response to dark patterns will succeed only if it ceases to treat the interface as a marginal compliance object and begins to treat it as the principal site of legal regulation. What follows is a synthesised set of recommendations, calibrated to the existing statutory architecture and designed to be operationally implementable within the constitutional and administrative-law constraints to which the Indian regulator is subject.

A. A Statutory Fairness-by-Design Mandate

The first and most consequential recommendation is the introduction of an explicit Fairness-by-Design mandate, modelled in structure on the Privacy-by-Design principle articulated by Cavoukian (2010) and codified in Article 25 of the GDPR (General Data Protection Regulation, 2016, art. 25). This mandate would require Data Fiduciaries and consumer-facing platforms to subject their user interfaces, prior to deployment and at periodic intervals thereafter, to an independent legal and human-computer-interaction audit. The audit would evaluate the interface against a published checklist derived from the CCPA Guidelines' enumerated patterns and the DPDP Act's quintuple consent criteria, and would generate a Compliance Certificate retained by the platform and producible on demand to either regulator (Powar, 2026).

The legislative vehicle for this mandate need not be a new statute. The DPDP Act, in Section 40, vests the Central Government with rule-making power that is amply sufficient to prescribe technical and procedural standards for the obtaining of consent, including standards for interface design (Digital Personal Data Protection Act, 2023, s. 40). The Consumer Protection Act, in Sections 94 and 101, vests cognate rule-making and regulation-making powers in the Central Government and the CCPA respectively (Consumer Protection Act, 2019, ss. 94, 101). A co-notified set of rules under both statutes, prescribing the Fairness-by-Design audit standard and a shared interface taxonomy, would harmonise the substantive obligation without legislative amendment.

B. The CCPA-DPBI Joint Task Force

The second recommendation is the constitution of a permanent Joint Task Force, formalised through a Memorandum of Understanding between the CCPA and the DPBI, with statutory recognition under the rule-making powers identified above. The Task Force should be vested with three operative functions. The first is coordinated investigation: where a complaint or referral relates to interface design, both regulators should be notified, evidence should be jointly gathered, and a coordinated investigative timeline should be agreed at the outset. The second is allocational guidance: the Task Force should issue non-binding guidelines on which regulator is the appropriate primary actor in particular categories of complaint, and on the circumstances in which simultaneous proceedings are appropriate. The third is penalty calibration: the Task Force should publish, in consultation with the Ministry of Law and Justice, non-binding guidance on the avoidance of cumulative penalty in cases where both regulators have proceeded to adjudication (Powar, 2026).

The constitutional propriety of such an arrangement deserves brief comment. The Task Force would not derogate from the statutory powers of either regulator; each retains its discretion to proceed under its own enabling statute. The Memorandum operates at the level of administrative practice, in the manner of the Memoranda of Understanding that the Reserve Bank of India and the Securities and Exchange Board of India have for many years concluded in respect of overlapping regulatory subjects (Reserve Bank of India, 2008). The constitutional concern identified in Part IV is thereby addressed not by statutory amendment but by administrative practice anchored in modest rule-making.

C. Mandatory Independent Audits and Transparency Reporting

The third recommendation supplements the Fairness-by-Design mandate with an obligation of annual transparency reporting. Platforms above a notified threshold of users—plausibly five million Indian users, calibrated to the Significant Data Fiduciary classification under Section 10 of the DPDP Act—should publish, in a prescribed format, the number of interface audits conducted, the patterns identified, the remedial steps taken, and the number of user complaints received in respect of interface design (Digital Personal Data Protection Act, 2023, s. 10). The model is the transparency reporting regime developed by the European Commission under the Digital Services Act and the analogous reporting obligations imposed on platforms by Article 24 (Digital Services Act, 2022, art. 24).

Transparency reporting carries a double dividend. It supplies the regulators with the empirical infrastructure they presently lack and which their constrained in-house capacity cannot independently generate; and it produces a reputational discipline on the platform that operates *ex ante*, prior to any enforcement action. The combination of audit-based compliance and transparency-based discipline is, in the EU experience, materially more effective than enforcement-based deterrence operating in isolation (European Commission, 2024).

D. Codification of Algorithmic Coercion as a Vitiating Factor

The fourth recommendation, more doctrinally ambitious, is the codification of algorithmic coercion as a recognised vitiating factor under Indian contract and data-protection law. The codification could proceed in the first instance through the issuance of joint interpretive guidance by the CCPA and the DPBI, articulating the architectural conditions under which consent obtained through a closed interface is to be presumed non-free. In the medium term, a legislative amendment to Section 14 of the Indian Contract Act, 1872, or the introduction of a free-standing provision in the DPDP Act through the rule-making power, would place the doctrine on its proper statutory footing (Powar, 2026).

E. Conclusion: Regulating the Code, Not Merely the Text

The central thesis of this paper has been that the convergence of deceptive design and vitiated consent is not an incidental overlap between two regulatory regimes but a structural feature of the platform-mediated economy. The CCPA Guidelines, 2023, and Section 6 of the DPDP Act, 2023, address the same transactional moment through different conceptual frames and with sharply asymmetric remedial inventories. The result, in the absence of doctrinal harmonisation and institutional coordination, is a regulatory blind spot through which the most sophisticated tech conglomerates can navigate by exploiting the seams between the two regimes.

The doctrinal correction is not, however, beyond the reach of the existing statutory architecture. The rule-making powers vested in the Central Government and the two regulators are amply sufficient to co-notify a Fairness-by-Design audit standard, to constitute a Joint Task Force, to require transparency reporting, and to issue interpretive guidance recognising algorithmic coercion as a vitiating factor. The intervention required is administrative imagination rather than legislative renovation.

The stakes of this intervention are not modest. India's Next Billion Users will encounter the digital economy not as sophisticated negotiators of terms of service but as users of interfaces designed by parties whose interests are asymmetric to their own. The protective ambition of the Consumer Protection Act, 2019, and the DPDP Act, 2023, can be realised in the practical experience of these users only if the legal system regulates the code of the interface and not merely the text of the policy. Doctrine has, in the years since Puttaswamy, supplied the language of dignitary autonomy; statute has, in 2019 and 2023, supplied the architecture of enforcement. What remains is the harder, quieter work of harmonisation—the work of ensuring that two regulators speaking the same descriptive language do so from a coordinated doctrinal vocabulary and a shared institutional discipline. The interface is the contract. The interface must, in consequence, be the object of law.

Footnotes

- [50] A. Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Information and Privacy Commissioner of Ontario, 2010).
- [51] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 25, codifying data protection by design and by default.
- [52] Digital Personal Data Protection Act 2023, s. 40, conferring rule-making power on the Central Government in respect of, inter alia, the manner of obtaining consent and the form of consent.
- [53] Consumer Protection Act 2019, ss. 94 (power of the Central Government to make rules) and 101 (power of the Central Authority to make regulations).
- [54] Reserve Bank of India–Securities and Exchange Board of India, *Memorandum of Understanding for Information Sharing and Coordinated Supervision* (May 2008), an Indian precedent for the inter-regulator coordination here proposed.
- [55] Digital Personal Data Protection Act 2023, s. 10, providing for the notification of Significant Data Fiduciaries on the basis of, inter alia, the volume of personal data processed and the risk to the rights of Data Principals.
- [56] Digital Services Act 2022, art. 24, imposing transparency reporting obligations on providers of intermediary services.
- [57] European Commission, *First Annual Report on the Application of the Digital Services Act* (Brussels, 2024) 18-26.
- [58] Indian Contract Act 1872, s. 14, in respect of which the proposed legislative amendment would codify algorithmic coercion as a recognised category alongside the existing five.
- [59] Justice K. S. Puttaswamy (Retd.) v. Union of India (n 15), per Chandrachud J, at [298]-[326], articulating the constitutional foundation of informational privacy on which the DPDP Act ultimately rests.
- [60] Powar, C., ‘The Convergence of Deceptive Design and Vitiating Consent’ (2026, this paper), recapitulating the structural argument for treating the interface as the proper object of Indian regulatory law.

References

- Article 29 Data Protection Working Party. (2018). *Guidelines on Consent under Regulation 2016/679* (WP259 rev.01). Brussels: European Commission.
- Bamberger, K. A., and Mulligan, D. K. (2015). *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. Cambridge, MA: MIT Press.
- Bhandari, V., and Sane, R. (2023). *A Critique of the DPDP Act, 2023* (NIPFP Working Paper). New Delhi: National Institute of Public Finance and Policy.
- Brignull, H. (2010). *Dark Patterns: User Interfaces Designed to Trick People*. darkpatterns.org.
- Cavoukian, A. (2010). *Privacy by Design: The 7 Foundational Principles*. Toronto: Information and Privacy Commissioner of Ontario.
- Central Consumer Protection Authority. (2023). *Guidelines for Prevention and Regulation of Dark Patterns*. Notification No. CCPA/Dark Patterns/2023, dated 30 November 2023. New Delhi: Department of Consumer Affairs.
- Cialdini, R. B. (2007). *Influence: The Psychology of Persuasion*. New York: HarperBusiness.
- Cohen, J. E. (2019). *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press.
- Consumer Protection Act, 2019 (Act No. 35 of 2019). New Delhi: Government of India.
- Department of Consumer Affairs. (2024). *Annual Report 2023-24*. New Delhi: Ministry of Consumer Affairs, Food and Public Distribution, Government of India.
- Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). New Delhi: Government of India.

European Commission. (2024). First Annual Report on the Application of the Digital Services Act. Brussels: European Commission.

European Data Protection Board. (2022). Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces. Brussels: EDPB.

Federal Trade Commission. (2022). Bringing Dark Patterns to Light (Staff Report). Washington, DC: FTC.

Federal Trade Commission. (2023). FTC v. Amazon.com Inc., Case No. 2:23-cv-00932 (W.D. Wash., filed 21 June 2023).

Hartzog, W. (2018). Privacy's Blueprint: The Battle to Control the Design of New Technologies. Cambridge, MA: Harvard University Press.

Indian Contract Act, 1872 (Act No. 9 of 1872). New Delhi: Government of India.

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

Kahneman, D., and Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 47(2), 263-291.

Luguri, J., and Strahilevitz, L. J. (2021). Shining a Light on Dark Patterns. *Journal of Legal Analysis*, 13, 43-109.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., and Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction*, 3 (CSCW), Article 81.

Mulla, D. F. (2018). *The Indian Contract and Specific Relief Acts* (15th ed.). Gurgaon: LexisNexis.

Powar, C. (2026). *The Convergence of Deceptive Design and Vitiating Consent*. Pune: D.E.S. Shri Navalmal Firodia Law College.

Regulation (EU) 2016/679 (General Data Protection Regulation), OJ L 119/1.

Regulation (EU) 2022/2065 (Digital Services Act), OJ L 277/1.

Reserve Bank of India. (2024). Payment System Indicators, Monthly Bulletin (March 2024). Mumbai: RBI.

Sunstein, C. R. (2020). Sludge Audits. *Journal of Risk and Uncertainty*, 36(2), 1-21.

Thaler, R. H., and Sunstein, C. R. (2008). *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New Haven: Yale University Press.