INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

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

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

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

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

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

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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

ISSN: 2582-6433

DARK PATTERNS AND ALGORITHMIC MANIPULATION: EXAMINING CONSUMER AUTONOMY, DIGITAL ETHICS, AND REGULATORY CHALLENGES IN THE CONTEMPORARY ONLINE ECOSYSTEM

AUTHORED BY - MHD USAM

ABSTRACT

The proliferation of AI has sharpened both the reach and the personalisation of 'dark patterns' interface and experience choices designed to nudge users towards decisions they would not otherwise make. This paper compares how India and the EU regulate such practices. Both jurisdictions share a basic diagnosis but diverge in regulatory philosophy, taxonomic breadth, enforcement architecture, and penalty deterrence. India's framework rests on the Consumer Protection Act 2019, the 2023 Guidelines for Prevention and Regulation of Dark Patterns, and the Digital Personal Data Protection Act 2023. It offers admirable definitional clarity but is undermined by jurisdictional fragmentation, non-binding illustrations, and penalties that barely register against the revenues of large platforms. The EU's 'digital design acquis' spanning the GDPR, the Unfair Commercial Practices Directive, the Digital Services Act, and the Digital Markets Actis principles-based and institutionally well-resourced, though not without its own fragmentation. Drawing on enforcement actions involving TikTok, Planet49, BookMyShow, IndiGo, and Flipkart, the paper proposes structural reforms for India: tiered data classification, fairness-by-design duties, turnover-based penalties, and mandatory algorithmic audits.

Keywords: Dark Patterns; Algorithmic Manipulation; Consumer Protection; GDPR; Digital Services Act; Consumer Protection Act 2019; Digital Personal Data Protection Act 2023; Comparative Law.

I. INTRODUCTION

India's digital marketplace has expanded at a pace that would have seemed implausible a decade ago. Internet connections grew from 25.15 crore in 2014 to 96.96 crore by April 2025a rise of over 285 per cent. The cost of mobile data fell from roughly ₹308 per gigabyte in 2014 to ₹9.34 by 2022, a drop of nearly 97 per cent. Cheap data has put a smartphone in almost every adult hand.

ISSN: 2582-6433

That expansion carries a quieter cost. Hundreds of millions of new usersmany with limited digital literacynow transact and socialise through interfaces whose neutrality cannot be assumed. What has emerged instead is a sophisticated set of design strategies known as 'dark patterns'. In their AI-augmented forms, these techniques draw on cognitive biases, behavioural data, and predictive models to steer users towards choices they would probably not make if fully informed.

Harry Brignull coined the term; Arunesh Mathur and colleagues gave it scholarly weight by cataloguing dark patterns across more than 11,000 shopping websites.[1] Colin Gray and colleagues offered a working definition: design strategies that 'advantage an online service by coercing, steering, or deceiving users into unintended and potentially harmful actions'.[2] AI-driven personalisation has since sharpened the concept further. Kadir Deligöz documents how machine learning enables 'privacy nudging'manipulating users into disclosing data through behavioural analysisalongside 'forced continuity', where churn-prediction models make cancellations deliberately harder.[3] Mark Leiser and Cristiana Santos describe a 'deceptive design visibility spectrum': from visible dark patterns identifiable by attentive users, to darker ones revealed only after the fact, to the 'darkest' patterns embedded deep in algorithmic architecture and effectively invisible to users and regulators alike.[4]

This paper compares the two most consequential regulatory responses: India's and the EU's. Part II sets out the conceptual framework. Part III surveys India's regulatory structure, and Part IV the EU's digital design acquis. Part V draws a comparative analysis, Part VI examines leading case studies, and Part VII identifies structural deficiencies and proposes reform.

II. CONCEPTUAL FRAMEWORK: DARK PATTERNS AND ALGORITHMIC MANIPULATION

A. Defining Dark Patterns

The literature converges on a core idea: dark patterns are interface choices that exploit fast, impulsive cognitionwhat behavioural economists call 'System 1'and in doing so override

[1]Arunesh Mathur et al., Dark Patterns at Scale: Findings from a Crawl of 11,000 Shopping Websites, 3(CSCW) Proc. ACM Hum.-Comput. Interact. 1, 1–2 (2019).
[2]Colin M. Gray et al., The Dark (Patterns) Side of UX Design, in Proc. 2018 CHI Conf. on Hum. Factors in Computing Sys. 534, 534 (2018).
[3]Kadir Deligöz, Consumer Manipulation with Artificial Intelligence: Dark Patterns and Hidden Techniques 41–52 (Ozgur Publications 2025).
[4]Mark R. Leiser & Cristiana Santos, Dark Patterns, Enforcement, and the Emerging Digital Design Acquis: Manipulation Beneath the Interface 4–7 (SSRN Working Paper, 2023).

ISSN: 2582-6433

what users would genuinely prefer. Mathur, Kshirsagar, and Mayer identify four recurring attributes. Dark patterns are *asymmetric* (they benefit the platform at the user's expense), *restrictive* (they narrow the choice architecture), *covert* (their operation is hidden), and *deceptive* (they create false beliefs about available options).[5]

Di Geronimo and colleagues found that 95 per cent of popular mobile applications contain at least one dark pattern, and that users cannot identify them unless explicitly primed to look.[6] That finding helps explain why disclosure-centred regulation tends to disappoint. Bongard-Blanchy and colleagues add a complementary point: 59 per cent of users in their survey recognised dark patterns yet still succumbed to them. As one participant put it, 'I am definitely manipulated, even when I am aware of it. It's ridiculous!'[7] Awareness, in other words, is not the same as resistance.

B. The Visibility Spectrum

Leiser and Santos identify three registers of manipulative design.[8] *Visible* dark patternspre-checked boxes, obstructive refusal options, false countdown timersare identifiable by attentive users or auditors. *Darker* dark patterns emerge only after the fact: hidden costs appearing at checkout, or unsubscribe flows requiring multiple screens and a phone call. The *darkest* patterns are embedded in system architecture or in non-deterministic algorithms invisible to users, hard for regulators to detect without code access, and often only surfaced through formal audit.

C. AI-Enhanced Dark Patterns and Explainability Pitfalls

AI converts dark patterns from static design choices into dynamic, continuously optimised influence systems. Three features distinguish AI-enhanced patterns from older counterparts: hyper-personalisation (targeting each user's specific vulnerability), continuous optimisation through reinforcement learning, and plausible deniability (since non-deterministic algorithms can produce manipulation without conscious intent, complicating legal frameworks that pivot on intent).

[5]Arunesh Mathur, Mihir Kshirsagar & Jonathan Mayer, What Makes a Dark Pattern… Dark? Design Attributes, Normative Considerations, and Measurement Methods, in Proc. 2021 CHI Conf. on Hum. Factors in Computing Sys. 1, 5–8 (2021).
[6]Linda Di Geronimo et al., UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception, in Proc. 2020 CHI Conf. on Hum. Factors in Computing Sys. 1, 9 (2020).
[7]"I Am Definitely Manipulated, Even When I Am Aware of It. It's Ridiculous!": Dark Patterns from the End-User Perspective, Kerstin Bongard-Blanchy et al., in Proc. ACM Designing Interactive Sys. Conf. 763, 770 (2021).
[8]Leiser & Santos, supra note 4, at 4–7.

ISSN: 2582-6433

Upol Ehsan and Mark Riedl draw a further distinction worth noting: between intentional dark patterns and 'explain ability pit falls' the unanticipated, harmful downstream effects of AI-generated explanations.[9] A common example is unwarranted trust in numerical AI outputs: users treat risk scores or match percentages as authoritative even when they cannot evaluate the underlying model. A framework aimed only at intentional deception will not reach these harms. More forward-looking regulation would require platforms to audit AI explanations for foreseeable misinterpretationtreating foreseeability as presumed where a documented pitfall is deployed without mitigation.

III. INDIA'S REGULATORY FRAMEWORK

A. The Consumer Protection Act 2019 and the 2023 Guidelines

India's primary instrument for regulating dark patterns is the Consumer Protection Act 2019 (CPA), which established the Central Consumer Protection Authority (CCPA) as the principal enforcement body. In November 2023, the CCPA issued the Guidelines for Prevention and Regulation of Dark Patternsprobably the world's most explicit statutory taxonomy of prohibited dark-pattern types.[10]

The 2023 Guidelines define a dark pattern as 'any practice or design that deceives, coerces, or misleads users to do something they did not intend or want to do; which results in a choice or an action by the user that is to the detriment of the user and to the advantage of the seller, service provider, or platform.' The definition is functionally sound. Its limitation is its emphasis on intentional deceptionlanguage that sits awkwardly when AI-generated manipulation operates without conscious intent.

Annexure I lists thirteen prohibited patterns: false urgency; basket sneaking; confirm shaming; forced action; subscription traps; interface interference; bait and switch; drip pricing; disguised advertisements; nagging; trick questions; SaaS billing; and rogue malwares. False urgency creates artificial scarcity to activate loss aversion ('Only 2 rooms left!'). Basket sneaking adds items or charges to a cart without express consent. Confirm shaming uses emotionally loaded language to discourage opt-outs ('No, I don't want to save money').[11] Drip pricing reveals fees incrementally, disclosing the true cost only at checkout.[12]

[9]Upol Ehsan & Mark O. Riedl, Explainability Pitfalls: Beyond Dark Patterns in Explainable AI, 11 Heliyon e41048, 3–5 (2024).
[10]Central Consumer Prot. Auth., Guidelines for Prevention and Regulation of Dark Patterns, F. No. J-25/3/2023-CCPA, § 3 (Nov. 30, 2023) (India) [hereinafter 2023 Guidelines].
[11]2023 Guidelines, supra note 10, Annex. I, ¶¶ 1–3.
[12]Sandeep Sharma & Ishita Sharma, Dark Patterns in a Bright World: An Analysis of the Indian Consumer Legal Architecture, 11 Int'l J. Consumer L. & Prac. 124, 130–33 (2023).

ISSN: 2582-6433

Violations attract penalties under Section 89 of the CPA: fines up to ₹10 lakh for first contraventions and ₹50 lakh for subsequent ones. These figures may deter smaller operators. For platforms whose annual revenues run into thousands of crores, they are not deterrents at all.

B. The Digital Personal Data Protection Act 2023

The Digital Personal Data Protection Act 2023 (DPDPA) creates what Aman Varma calls a 'dual liability exposure' for dark patterns.[13] A pattern that compromises consent validity under Section 4(1)(a)which requires consent to be specific, free, and informedconstitutes a DPDPA violation in its own right, attracting penalties up to ₹250 crore per violation. Confirm shaming, nagging, trick questions, interface interference, and forced action can each independently impair valid consent.

The Act has real structural weaknesses. Bisht and Sreenivasulu describe its notice requirements as 'sketchy', and note the absence of dedicated provisions for the right to be forgotten and data portability.[14] Tandon and Gupta press the point further: the DPDPA's broadly uniform approach to personal datatreating trivial and sensitive data alikesits uneasily with the constitutional proportionality doctrine articulated in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[15]

C. Jurisdictional Fragmentation

A single incidentbasket sneaking, invalid-consent data collection, and self-preferencing by a dominant platformcan trigger concurrent jurisdiction of the CCPA, the Data Protection Board of India, and the Competition Commission of India, each before a separate authority. *Bharat Matrimony v. Google Inc.* illustrates the cost. The CCI initially declined privacy-related claims as competition matters before eventually recognising data as a non-price competition parametera process that took years and imposed significant litigation costs on complainants throughout.[16]

[13]Aman Varma, The Legal Perils of Dark Patterns in India: Intersection Between Data Privacy and Consumer Protection, SCC Online (Apr. 2025).
[14]Ajay Kumar Bisht & N.S. Sreenivasulu, Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act 2023 87–91 (2024).
[15]Usha Tandon & Neeraj Kumar Gupta, Informational Privacy in the Age of Artificial Intelligence: A Critical Analysis of India's DPDP Act, 2023, 6 Legal Issues Digital Age 87, 95–97 (2025); see Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶ 325 (India).
[16]Renu Gupta & Akshat Bhushan, Looking at Dark Patterns in Light of the Competition Law in India, Oxford Bus. L. Blog (Nov. 30, 2021); see Bharat Matrimony v. Google Inc., Case No. 7 of 2012 (CCI 2018).

ISSN: 2582-6433

IV. THE EUROPEAN UNION'S DIGITAL DESIGN ACQUIS

A. The GDPR

The General Data Protection Regulation (GDPR) addresses dark patterns primarily through its consent requirements. Article 7 demands that consent be 'freely given, specific, informed and unambiguous', with withdrawal as easy as its provision. Recital 32 expressly rules out pre-ticked boxes and silence as valid consent mechanisms. In *Planet49,* the Court of Justice gave those provisions real force, holding that a pre-ticked checkbox does not constitute valid consent because 'inaction cannot be construed as an active affirmative indication of agreement'.[17]

Article 25's obligation of 'data protection by design and by default' goes further: controllers must configure defaults in the most privacy-protective manner available. That affirmative design duty is structurally the antithesis of the dark-pattern instinct. Yet compliance has not followed automatically: Nouwens and colleagues found that nearly 90 per cent of the top 10,000 UK websites' cookie consent dialogues contained dark patterns failing minimum European requirements.[18] Substantive obligations, on their own, do not change platform behaviour at scale.

B. The Unfair Commercial Practices Directive

Directive 2005/29/EC prohibits misleading and aggressive commercial practices in business-to-consumer relationships. Annex I's blacklist captures several dark-pattern types outright, including representations of artificial scarcity. General prohibitions on misleading actions and omissions then operate as a principles-based catch-all for the darker patterns that no specific entry covers.

C. The Digital Services Act

The Digital Services Act (DSA), Regulation (EU) 2022/2065, is the EU framework's most direct legislative response. Article 25 prohibits online platforms from designing or operating their interfaces in ways that 'deceive or manipulate' users or 'materially distort' their capacity to make free and informed decisions. Specifically prohibited practices include giving disproportionate visual prominence to certain choices, repeatedly asking users to revisit a

[17]Council Regulation 2016/679, art. 7, 2016 O.J. (L 119) 1, 37 (EU); Planet49 GmbH v. Bundesverband der Verbraucherzentralen, Case C-673/17, ECLI:EU:C:2019:801, ¶ 52 (Oct. 1, 2019).
[18]Midas Nouwens et al., Dark Patterns After the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence, in Proc. 2020 CHI Conf. on Hum. Factors in Computing Sys. 1, 7–9 (2020).

ISSN: 2582-6433

decision already made, and making cancellation harder than subscription.[19] Enforcement against Very Large Online Platforms vests directly in the European Commission, and Article 40 obliges those platforms to grant regulators and vetted researchers access to their algorithmic systems for compliance auditingthe technical infrastructure needed to investigate the darkest patterns.

D. The Digital Markets Act and the AI Act

The Digital Markets Act targets large gatekeepers controlling key digital infrastructure, imposing ex ante obligations including bans on self-preferencing and interface manipulation that subverts user autonomy. The EU AI Act prohibits systems that deploy 'subliminal techniques beyond a person's consciousness' or exploit the vulnerabilities of specific groups to cause material harm. Devetzis and Samaras argue that the AI Act matters chiefly as regulatory plumbingsupplying the technical infrastructure needed to address the darkest patterns that consumer and data protection instruments alone cannot reach.[20]

V. COMPARATIVE LEGAL ANALYSIS

A. Taxonomic Approach: Enumerated Rules versus Principles

The deepest divergence between the two frameworks is taxonomic. India's 2023 Guidelines enumerate thirteen specifically prohibited patterns. Article 25 of the DSA prefers a principles-based prohibition supplemented by illustrative examples. Each approach has its pathologies.

The enumerated approach gives prosecutors and courts a useable vocabulary. The price, in India's case, is that Annexure I is explicitly stated to be 'illustrative and non-binding'a qualification that lets platforms argue novel patterns fall outside any enumerated type. The principles-based approach avoids that rigidity but requires case-by-case elaboration before it offers equivalent precision. India's taxonomy is also incomplete: privacy zuckering, friend spam, fake social proof, and price comparison prevention are all documented in the academic literature and addressed in other jurisdictions, yet none appears in the 2023 Guidelines.

B. Consent Framework Divergence

The most consequential jurisprudential difference lies in how the frameworks treat

[19]Regulation (EU) 2022/2065, art. 25, 2022 O.J. (L 277) 1, 47 (EU).
[20]Dimitrios Devetzis & Simos Samaras, Consumer Protection Safeguards After the AI Act, 13 Persps. L. & Pub. Admin. 298, 305 (2024).

ISSN: 2582-6433

informed consent. The GDPR pairs its rights-based philosophy with an affirmative design duty under Article 25 to configure defaults in the most privacy-protective manner available. That reversal of the default presumption is structurally transformative: dark patterns are, by definition, inconsistent with a default-protective design obligation.

The DPDPA's approach is comparatively thinner. Its notice requirements fall short of the GDPR's layered disclosure obligations. Its 'deemed consent' provisions in Section 7 are vague enough to be open to manipulation by platforms dressing dark-pattern-induced actions as legitimate consent. The absence of both data portability and a comprehensive right to erasure leaves subscription-trap and forced-continuity patterns structurally unaddressed.

C. Penalty Calibration and Deterrence

A regulatory framework lives or dies by the deterrent force of its penalties. The GDPR allows fines of up to €20 million or 4 per cent of global annual turnover, whichever is higher, for the most serious violations. The CNIL's fines of €60 million and €40 million against Google show that framework operating at scale. The DSA provides for fines of up to 6 per cent of global annual turnover for VLOP violations.

India's penalty structure does not approach those levels. Maximum CPA fines of ₹50 lakh represent roughly 0.05 per cent of a large platform's annual revenuea rounding error. The DPDPA's ₹250 crore ceiling is a meaningful improvement, but it still falls short of turnover-based calibration and below the GDPR's 4 per cent benchmark.

VI. CASE STUDIES IN DARK PATTERN ENFORCEMENT

A. Default Settings as Dark Patterns: TikTok (DPC 2023)

In *In re TikTok Technology Ltd.*, the Irish Data Protection Commission enforced the GDPR against TikTok for processing personal data of users aged 13 to 17. TikTok's 'public-by-default' account settings rendered child users' videos, comments, and profiles globally accessible without adequate transparency or protective defaults.[21] The case shows how a default setting can itself function as a structural dark pattern. By making accounts public by default, TikTok leveraged status-quo bias to achieve mass-scale privacy invasion without any single overt manipulative act. The decision treats 'protection by design and default' not as aspirational language but as an enforceable requirement, particularly where vulnerable users are involved.

[21]In re TikTok Technology Ltd., Decision No. IN-21-9-1, ¶¶ 8.1–8.6 (Data Prot. Comm'n, Ire., Sept. 1, 2023).

ISSN: 2582-6433

B. Preselection as Invalid Consent: Planet49 (CJEU 2019)

In *Planet49,* the Court of Justice held that a pre-ticked checkbox cannot constitute valid consent under Article 7 of the GDPR. A user's failure to uncheck a box cannot be construed as active agreement.[22] The judgment outlawed preselection as a consent mechanism across the EU and established a broader principle: any pre-selected optionfor a subscription, for data sharing, for an ancillary servicemust be affirmatively chosen by the user to count as valid consent. The implications extend well beyond cookie banners.

C. Basket Sneaking and Drip Pricing: Indian Consumer Commission Cases

The CCPA took action against BookMyShow for automatically adding a ₹1 'BookASmile' donation to ticket purchases via a pre-ticked checkbox.[23] Users who did not actively uncheck the box found a charge added without affirmative consentclassified as basket sneaking under the 2023 Guidelines. The conduct directly mirrors the preselection violation recognised in *Planet49*.

In *Ashwani Chawla v. Flipkart Internet Pvt. Ltd.,* the State Consumer Disputes Redressal Commission used the 2023 Guidelines as interpretive tools to characterise specific platform conduct as dark patterns. Flipkart had imposed an 'offer handling fee' alongside a separately charged shipping fee (drip pricing), and had delivered a used mobile phone described as new (bait-and-switch). It is the first significant instance of an Indian judicial body formally citing the 2023 Guidelines to identify dark patterns, establishing them as live interpretive instruments in consumer disputes.

D. Confirm Shaming: CCPA Action against IndiGo

IndiGo Airlines deployed confirm shaming by presenting its seat-selection opt-out as 'No, I will take the risk'leveraging fear and guilt to push users towards services they had not chosen. After regulatory scrutiny, the airline replaced the language with a neutral formulation. The financial penalty was modest, but the behavioural change matters and represents a form of deterrence that fines alone do not capture. Real-time product changes driven by regulatory attention are, in some respects, more valuable than an after-the-fact fine.

[22]Planet49 GmbH v. Bundesverband der Verbraucherzentralen, Case C-673/17, ECLI:EU:C:2019:801, ¶ 52 (Oct. 1, 2019).
[23]CCPA Order against BookMyShow, Cent. Consumer Prot. Auth. (India 2024); Leiser & Santos, supra note 4, at 18.

ISSN: 2582-6433

VII. STRUCTURAL DEFICIENCIES AND REFORM RECOMMENDATIONS

A. Structural Deficiencies in the Indian Framework

Four structural weaknesses limit the effectiveness of India's current dark-pattern regime. First, the Annexure I taxonomy is non-binding, weakening deterrence and enabling platform arguments that novel patterns fall outside enumerated types. Second, the taxonomy is materially incomplete: privacy zuckering, friend spam, fake social proof, and price comparison prevention are each documented in the academic literature and addressed in other jurisdictions. Third, concurrent CCPA, Data Protection Board, and CCI jurisdiction over overlapping aspects of a single incident imposes prohibitive transaction costs on complainants and yields inconsistent outcomes. Fourth, fixed-ceiling penalties that amount to a rounding error against a large platform's revenue cannot generate genuine deterrence.

B. Recommendations for Reform

1. **Tiered data classification.** The DPDPA's uniform approach should give way to a tiered classification hierarchy in which protection rises with sensitivity. Biometric, health, financial, and children's data should attract the highest tier, including an express prohibition on dark patterns in consent flows. This reflects the proportionality doctrine in *Puttaswamy*: a one-size-fits-all rule is constitutionally and practically inadequate when the same consent pattern may secure either a newsletter preference or facial-recognition data.[24]
2. **Binding taxonomy with a principles-based catch-all.** The non-binding character of Annexure I should be replaced by a binding principles-based definition, supplemented by a regularly updated annex with binding presumptive force. The catch-all should expressly capture privacy zuckering, friend spam, fake social proof, and price comparison prevention, combining India's current taxonomic specificity with the DSA's scalability.
3. **Dual liability integration.** The 2023 Guidelines should be formally integrated with the DPDPA so that dark patterns impairing consent under Section 4(1)(a) automatically attract DPDPA liability. Confirm shaming, nagging, trick questions, interface interference, and forced action should each be designated, in terms, as consent-

[24]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, ¶¶ 310–325 (India); Tandon & Gupta, supra note 15, at 95.

ISSN: 2582-6433

impairing mechanisms, creating automatic dual liability wherever they appear in data-collection contexts.

4. **Fairness-by-design obligations and mandatory algorithmic audits.** Following the GDPR Article 25 model, platforms above a defined user-base threshold should face affirmative 'fairness by design' duties, requiring defaults configured in the most privacy- and consumer-protective manner available, together with periodic UI/UX and algorithmic audits submitted to a designated regulator. Published audit summaries would create a transparency infrastructure broadly analogous to the DSA's algorithmic transparency requirements for very large online platforms.
5. **Turnover-based penalties.** Fixed-ceiling penalties should be supplemented by turnover-based fines modelled on Article 83 of the GDPR. That calibration is necessary if penalties are to deter operators for whom present maximums are a predictable and trivial cost of doing business.
6. **Coordinated enforcement mechanism.** Jurisdictional fragmentation between the CCPA, the CCI, and the Data Protection Board of India should be resolved through a coordinated enforcement mechanism that designates a primary authority for digital dark-pattern complaints, with formal inter-agency cooperation protocols ensuring that incidents implicating consumer protection, data protection, and competition are investigated holistically and resolved through coordinated action.

VIII. CONCLUSION

Dark patterns are a systemic market failure: the deliberate engineering of digital environments to override consumer autonomy at scale, drawing on cognitive bias, information asymmetry, and algorithmic personalisation to extract value from users without and often against their genuine preferences. The empirical evidence is fairly unambiguous. Users know they are being manipulated and still cannot resist; platforms deploy these techniques because they work; and current regulation in both India and the EU, while meaningful, remains structurally insufficient against the darkest patterns embedded in algorithmic architecture.

The comparison reveals convergence in intent and divergence in structure. Both jurisdictions share the foundational concern that digital interface design has become a vehicle for systematic manipulation. They diverge in the depth, enforceability, and institutional architecture of their responses. The EU's digital design acquis supplies the more robust frame work affirmative design duties, principles-based prohibitions, mandated algorithmic transparency, turnover-based penalties, and a coordinated enforcement architecture capable of

ISSN: 2582-6433

probing the darkest patterns.

For India, the path forward is reasonably clear in principle, if difficult in execution. The 2023 Guidelines are a real regulatory achievement particularly in their definitional clarity and formal citation in judicial proceedings but they are insufficient as currently drafted. The reforms proposed here would bring India's framework closer to the substantive protection that its vast and disproportionately vulnerable digital population requires.

The ultimate normative justification for that programme rests on the constitutional foundation laid down in *Puttaswamy*: decisional privacy the right to make choices free from coercionis an aspect of the fundamental right to privacy under Article 21 of the Constitution. An interface that coerces a user through confirm shaming or forced action does not merely contravene a consumer-protection guideline. It can infringe a fundamental right, with correspondingly stronger remedial implications. The regulation of dark patterns is not only a consumer-protection matter. It is a constitutional one.