The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

SELF-CERTIFICATION AND THE STRUCTURE OF CONSUMER PROTECTION: A CRITICAL STUDY OF INDIA'S DARK PATTERN REGIME

~ Gyan Prakash Upadhyay & Vaibhav Mewada

I. Introduction: The Regulatory Paradox

On 5 June 2025, the Central Consumer Protection Authority directed every e-commerce platform operating in India to audit itself.[1] The instruction was unusual chiefly in its candour. Two years after the CCPA had prohibited thirteen categories of manipulative interface design under the Guidelines for Prevention and Regulation of Dark Patterns, 2023,[2] the regulator did not announce a further round of platform-specific inspections. It asked platforms to examine their own interfaces and report what they found.

By November 2025, twenty-six platforms had done so.[3] Flipkart, Myntra and Walmart India engaged Deloitte for third-party review; several others submitted single-paragraph assurances with no stated methodology.[4] Amazon the platform most frequently named in consumer complaints did not file until February 2026, three months after the twenty-six-platform list had already been publicised as a governmental success.[5] Independent testing over the same window found that most platforms declaring themselves free of dark patterns still displayed at least one

---

[1]Central Consumer Protection Authority, *Advisory in Terms of the Consumer Protection Act, 2019 on Self-Audit by E-Commerce Platforms for Detecting Dark Patterns on their Platforms* (5 June 2025) F. No. CCPA-1/1/2023-CCPA, available at doca.gov.in.

[2]*Guidelines for Prevention and Regulation of Dark Patterns, 2023*, F. No. CCPA-1/1/2023-CCPA, notified 30 November 2023 under s 18, Consumer Protection Act 2019.

[3]Ministry of Consumer Affairs, Food and Public Distribution, '26 Leading E-Commerce Platforms Declare Compliance with Self-Audit to Eliminate Dark Patterns' (Press Information Bureau, 20 November 2025) Release ID 2191948.

[4]MediaNama, 'Dark Pattern Audits of 18 E-Comm and Q-Comm Apps Released' (21 November 2025).

[5]MediaNama, 'Amazon App Shows Dark Patterns Despite CCPA Filing' (10 April 2026).

prohibited practice.[6] Even the basic count could not be stated consistently: the CCPA's press release recorded twenty-six; a Right to Information response filed the same week recorded twenty-five; only eighteen declarations were ever made public; and a citizen-audit organisation tracking the exercise referred to twenty-three.[7] Add Amazon's later filing and commentary understandably arrives at twenty-seventhough no verifiable official document appears to use that figure, and the true count depends on which list, and which date, one treats as authoritative.[8]

This numerical confusion is not an administrative footnote to the story; it is the story. The Consumer Protection Act, 2019 vests the CCPA with power to investigate, recall, penalise and prosecute.[9] Confronted with hundreds of platforms whose interfaces change continuously through routine experimentation, the CCPA has chosen to supplement that architecture with a process under which platforms audit their own compliance and declare the result. This essay asks whether that delegation is defensible not whether dark patterns should be prohibited, a question the 2023 Guidelines already answered, but whether detection of a technologically fluid, commercially profitable form of manipulation can be credibly entrusted to the entities that design the interface, profit from it, and alone hold the data needed to test it.

This essay argues that the June 2025 advisory is a rational but structurally incomplete response to the informational limits of command-and-control enforcement. Self-audit narrows the CCPA's information deficit; it does not resolve the platform's conflict of interest, and nothing in the present architecture obliges it to. What is missing is institutional design: a tiered framework of *regulated* self-audit, combining continuous internal review with independent audit for high-reach platforms and retained, risk-based verification power in the CCPA broadly the direction in which the European Union has moved around the Digital Services Act. Self-

[6] MediaNama, 'What Gaps Do Dark Pattern Filings the CCPA Received Reveal?' (26 November 2025), reporting a LocalCircles survey conducted June–September 2025.
[7] ibid; MediaNama, 'RTI Shows 25 Platforms Filed Dark Pattern Audits, But None Public' (21 November 2025); PIB Release ID 2191948 (n 3); MediaNama, 'Amazon App Shows Dark Patterns Despite CCPA Filing' (n 5) (LocalCircles referring to 23 platforms under test as of January 2026).
[8] The author could not locate an official CCPA/PIB document explicitly recording a total of 27 platforms as of the date of writing. The figure most plausibly represents the original 26 (PIB Release ID 2191948, n 3) plus Amazon's later filing (n 5), but this arithmetic is inferred, not confirmed, and should be independently verified against the CCPA/DoCA self-audit portal (doca.gov.in/ccpa) or a subsequent parliamentary reply before the essay is finalised for submission.
[9] Consumer Protection Act 2019, ss 10, 18, 20–22.

audit is a legitimate first instrument of compliance; it is not, without more, a credible substitute for enforcement.

II. From Manipulative Design to a Legal Wrong

The Consumer Protection Act, 2019 does not use the phrase 'dark pattern'. It captures the conduct derivatively, through the definition of 'unfair trade practice' in Section 2(47) any practice adopting an unfair or deceptive method to promote the sale of goods or services[10] and through the CCPA's power under Section 21 to act against false or misleading advertisements.[11] The CCPA is itself a creature of Section 10, established because the pre-existing three-tier consumer commission structure, built for individual grievance redressal, had no capacity for class-wide, proactive market regulation.[12] Section 18 supplies that capacity, including, under Section 18(2)(l), the power to issue guidelines to prevent unfair trade practices and protect consumer interest.[13]

It was under this power that the CCPA notified the Guidelines for Prevention and Regulation of Dark Patterns, 2023 on 30 November 2023.[14] The Guidelines define a dark pattern as a design practice that misleads or tricks users into unintended action by 'subverting or impairing the consumer autonomy, decision making or choice', and treat such conduct as a misleading advertisement, an unfair trade practice, or a violation of consumer rights.[15] Annexure I lists thirteen specified patterns 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[16] expressly as illustrations, leaving the CCPA room to characterise new interface techniques as they emerge.

Two features of this design matter here. First, the Guidelines create no free-standing penalty; a violation is actionable only by routing it through the pre-existing machinery of Sections 20, 21, 88 and 89 recall, civil penalty for misleading advertisement, and criminal liability for

[10]Consumer Protection Act 2019, s 2(47).
[11]ibid, s 21.
[12]ibid, s 10 and ss 28–58 (District, State and National Consumer Disputes Redressal Commissions).
[13]ibid, s 18(2)(l).
[14]*Guidelines for Prevention and Regulation of Dark Patterns 2023* (n 2), cl 1.
[15]ibid, cl 2 (definition of 'dark patterns').
[16]ibid, Annexure I.

defying a CCPA direction.[17] They function less as an offence in their own right than as an interpretive schedule, telling the regulator and the consumer commissions what a dark pattern looks like so that Sections 2(47) and 21 can be applied to it. Second, despite this indirection, the instrument still binds. The Delhi High Court's 2025 decision in *National Restaurant Association of India v Union of India* on a different CCPA guideline, on service charges, but directly addressing the legal character of such guidelines held that the CCPA 'is not merely a recommendatory or advisory body'.[18] Read together, the 2023 Guidelines and *NRAI* establish that Indian dark pattern regulation, though implemented through a soft instrument, rests on a hard statutory foundation: a platform disregarding the Guidelines is not disregarding a suggestion but courting liability under a penal statute.

III. From Enforcement to Self-Audit: The 2025 Intervention

For roughly eighteen months after the Guidelines took effect, CCPA enforcement followed a conventional pattern: individual notices against specific platforms for specific practices BookMyShow, over a pre-ticked contribution to its 'BookASmile' charity,[19] and cab-aggregators Uber, Ola and Rapido, over an 'advance tip' feature treated as forced action.[20] This was command-and-control regulation working as designed complaint, investigation, direction, compliance but visibly failing to keep pace with the problem's scale: an independent LocalCircles survey found that ninety-seven per cent of major online platforms deployed at least one prohibited practice.[21]

The 5 June 2025 advisory was the CCPA's answer to that gap. Issued after a high-level stakeholder meeting convened by the Department of Consumer Affairs in May 2025,[22] it

[17]Consumer Protection Act 2019, ss 20, 21, 88, 89; see also 'CCPA Issues Guidelines for Prevention and Regulation of Dark Patterns, 2023 – Effective 30 November 2023' (Lexology, 4 December 2023), noting that the Guidelines specify no independent penalty of their own.

[18]National Restaurant Association of India & Ors v Union of India & Anr, WP(C) 10683/2022 (Delhi HC, 28 March 2025) (Prathiba M Singh J). The decision concerns the CCPA's 2022 guidelines on service charges, not the dark pattern Guidelines, but is relied on here for its general holding on the legal character of CCPA guidelines.

[19]'Dark Patterns in Digital Platforms: India's Rules & Guidelines' (Neeti Niyaman, 10 September 2025), reporting a CCPA notice to BookMyShow in February 2025 over a pre-ticked contribution to its 'BookASmile' initiative; this date should be independently verified against the CCPA's own order.

[20]Business Standard, 'Self-Audit within 3 mths: CCPA's Advisory to Ecom Firms on Dark Patterns' (7 June 2025), reporting CCPA notices to Uber, Ola and Rapido over an 'advance tip' feature.

[21]MediaNama, 'Dark Pattern Audits of 18 E-Comm and Q-Comm Apps Released' (n 4).

[22]AZB & Partners, 'The End of the Pre-Ticked Box? CCPA's Latest Step Towards Protecting Consumers' (30 June 2025), noting the high-level stakeholder meeting of 28 May 2025 convened by the Department of Consumer Affairs.

directed all e-commerce platforms to complete a self-audit within three months and, in markedly softer language, 'encouraged' them to submit a self-declaration of compliance.[23] It also invoked Rule 4(9) of the Consumer Protection (E-Commerce) Rules, 2020, which requires explicit, affirmative consumer consent and bars mechanisms such as pre-ticked boxes, giving the self-audit a concrete, testable design requirement to anchor itself to.[24] Tellingly, the advisory prescribes no audit methodology, no reporting template and no verification step, and leaves unclear whether the declaration must even be filed with the CCPA rather than merely displayed on the platform's own site.[25]

This choice reflects a real institutional constraint: the Authority could not feasibly test every platform's interface for thirteen categories of design practice that are, by nature, embedded in code, contingent on user segment, and subject to continuous experimentation. The platform already holds this information as an ordinary incident of running its business the same A/B-testing infrastructure that produces a dark pattern also produces the data needed to detect one. This is the logic of what regulatory scholarship calls *enforced self-regulation*: the state fixes the substantive standard and reserves the power to inspect and penalise, while delegating the operational task of monitoring to the regulated entity.[26] It is a rational answer to an acute information asymmetry and, without more, a delegation of the detection function to the party with every incentive to under-detect.

IV. The Credibility Problem of Platform Self-Certification

The distinction between self-regulation, self-audit, self-certification, co-regulation and responsive regulation is not semantic; each allocates the burden of verification differently. Pure self-regulation would let industry set its own standard; that is not India's position, since the standard the thirteen named patterns is fixed entirely by the CCPA. What the 2025 advisory delegates is narrower: the audit function, testing one's own conduct against an externally set standard, and the certification function, publicly declaring the result. Co-regulation typically preserves a standing role for the regulator or an accredited third party in verifying that self-assessment. Responsive regulation, in Ayres and Braithwaite's account, begins with persuasion

[23]Advisory (n 1); Chambers and Partners, 'Central Consumer Protection Authority Advisory on Self-Audit' (17 June 2025).
[24]Consumer Protection (E-Commerce) Rules 2020, r 4(9); Chambers and Partners (n 23).
[25]Chambers and Partners (n 23), noting the advisory's ambiguity on whether the declaration must be filed with the CCPA or merely displayed on the platform's own site.
[26]Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) ch 4 (describing 'enforced self-regulation').

and self-monitoring and escalates up an enforcement pyramid as compliance fails.[27] India's advisory borrows the vocabulary of responsive regulation but lacks its defining feature a trigger, short of a fresh complaint, for the CCPA to escalate once self-audits prove unreliable. What remains is closer to administrative self-reporting: platforms tell the regulator what they found, and the regulator publicises the aggregate.

The difficulty is structural, not moral. The party holding the deepest information about an interface its conversion-optimised checkout, its cancellation funnel, its personalised nudges is also the party whose revenue depends on that interface performing well, where 'performing well' and 'manipulating the user' are often the same design choice viewed from opposite ends. A self-audit asks a platform to act simultaneously as investigator, interpreter of an admittedly non-exhaustive standard, and beneficiary of a favourable finding. The advisory prescribes no methodology, so an internal review by the very product team responsible for the interface satisfies its letter; it requires no disclosure of what was tested, so 'self-audit conducted; platform free from dark patterns' the operative sentence in most published declarations is unfalsifiable on its face.[28]

The evidence bears this out. Of the twenty-six platforms declaring full compliance in November 2025, independent testing found that most continued to display at least one prohibited pattern; by January 2026, LocalCircles found every major platform but one non-compliant.[29] The CCPA itself later issued clarification notices to fifteen platforms several of which had filed a clean declaration weeks earlier for continuing to display the very practices they had certified as absent.[30] Amazon's declaration, filed after a five-month extension, claimed only 'substantial conformity', disclosed no methodology and no interface changes, and its app was independently found to retain dark patterns soon afterward.[31] Parliament was told in 2026 that total penalties recovered across the entire enforcement effort the Guidelines, the advisory, and every subsequent notice amounted to roughly ₹20 lakh, the largest single penalty being ₹7 lakh against Zepto.[32] Set against estimated annual consumer losses running into tens

[27]ibid, ch 2 (the responsive regulation enforcement pyramid).
[28]PIB Release ID 2191948 (n 3), reproducing the operative sentence of most published declarations.
[29]MediaNama (n 6); MediaNama (n 5) (reporting the January 2026 LocalCircles finding that all major platforms except one remained non-compliant).
[30]MediaNama, 'Amazon App Shows Dark Patterns Despite CCPA Filing' (n 5), reporting CCPA clarification notices issued to 15 platforms between 24 and 28 November 2025.
[31]ibid.
[32]Outlook Business, 'Inside India's Dark Pattern Crackdown: Why Zepto, BookMyShow and Others Are Under CCPA Scanner' (6 August 2026), reporting a Rajya Sabha written reply of the Minister of State, Consumer

of thousands of crores,[33] the self-audit exercise has generated declarations at a scale the CCPA could never have achieved through direct inspection but has not been shown to have generated compliance. The uncertainty over how many platforms even filed is, in this light, a small working model of the larger problem: a verification architecture that cannot say with confidence whether eighteen, twenty-three, twenty-five, twenty-six or twenty-seven platforms complied has not built the capacity to know whether they told the truth.

V. Lessons from Comparative Regulatory Models

The European Union confronts the identical asymmetry a regulator that cannot match platform scale and has moved toward, not away from, independent verification. Article 25 of the Digital Services Act prohibits platforms from designing interfaces that 'deceive or manipulate' users or materially distort their ability to make free, informed decisions, language Recital 67 explicitly links to dark patterns.[34] Crucially, the DSA does not stop at self-assessment: very large platforms those exceeding forty-five million average monthly users must conduct an annual risk assessment under Article 34 and commission an *independent* audit under Article 37, performed by an external auditor under a Commission delegated regulation and reported to the Commission and national regulators.[35] Self-assessment survives, but embedded in a structure where an outside party checks it imperfectly: because the audited platform selects and pays its own auditor, the platform X simply replaced a critical first auditor with a more accommodating one the following cycle, a reminder that independent audit narrows, but does not eliminate, a platform's capacity to shape its own verification.[36]

The EU's consumer-law track offers a sharper contrast still. Rather than relying on platform declaration, the Consumer Protection Cooperation Network coordinated by the Commission across member-state authorities ran its own sweep of 399 retail websites in 2022, found dark patterns on roughly forty per cent, and contacted the offending traders directly to demand

Affairs, Food and Public Distribution. The original parliamentary reply should be independently verified via sansad.in before submission.

[33] ibid, citing Datum Intelligence, 'Dark Patterns in India's Online Marketplaces' (as reported in Business Standard); the underlying report was not independently accessed and its figures should be verified before reliance.

[34] Regulation (EU) 2022/2065 (Digital Services Act), art 25 and recital 67.

[35] ibid, arts 33–34 and 37; Commission Delegated Regulation (EU) 2023/2777 of 25 October 2023 supplementing Regulation (EU) 2022/2065 as regards rules on the performance of audits for very large online platforms and very large online search engines.

[36] DSA Observatory, 'What are DSA Audits Doing for Systemic Risk Enforcement? The Case of X' (19 December 2025).

rectification.[37] A coordinated regulatory complaint over Amazon's Prime cancellation flow led the company to agree, under direct Commission engagement, to cut its EU cancellation process to two clicks the same company that, in India eighteen months later, filed a five-month-delayed declaration of 'substantial conformity' that independent testing found wanting.[38] Holding the platform constant across both cases is instructive: where the regulator tested the interface and negotiated a specific remedy, the interface changed; where the platform was asked only to test and declare, it did not, at least not verifiably. The Court of Justice's ruling in *Planet49* that a pre-ticked consent box can never constitute valid consent, reached through binding adjudication rather than platform attestation anticipated, by six years, the identical prohibition India would write into Rule 4(9) and the 2023 Guidelines.[39] The Union's own trajectory confirms the diagnosis: the forthcoming Digital Fairness Act, expected in late 2026, exists because the Commission's own evaluation found voluntary compliance still inadequate its answer to weak self-monitoring has been more independent oversight, not more delegated trust.[40] None of this recommends importing the DSA wholesale; India's market includes sellers far smaller than a designated very large platform, for whom a mandatory annual external audit would be disproportionate. The transferable insight is narrower: verification credibility scales with independence, best achieved not by choosing between self-audit and enforcement but by calibrating which mechanism governs which tier of the market.

VI. Toward a Verified Self-Audit Framework for India

A workable model should preserve self-audit as the default mechanism for most platforms while correcting four defects the 2025 advisory leaves open: no prescribed methodology, no independent check for high-risk platforms, no consequence for a false declaration, and no defined trigger for escalation. None of this needs new legislation; it needs the CCPA to connect instruments the Act already contains into a single, tiered sequence.

[37]European Commission, 'Consumer Protection: Manipulative Online Practices Found on 148 out of 399 Online Shops Screened' (Press Release, 30 January 2023).
[38]European Commission, 'Consumer Protection: Amazon Prime Changes its Cancellation Practices to Comply with EU Consumer Rules' (Press Release, 1 July 2022); MediaNama (n 5).
[39]Case C-673/17 *Bundesverband der Verbraucherzentralen und Verbraucherverbände v Planet49 GmbH* [2019] ECLI:EU:C:2019:801 (CJEU, Grand Chamber, 1 October 2019); Consumer Protection (E-Commerce) Rules 2020, r 4(9).
[40]European Commission, '2030 Consumer Agenda' (19 November 2025); European Parliament, Legislative Train Schedule, 'Digital Fairness Act', indicating a Commission proposal expected in Q4 2026 (accessed September 2026).

*Firstly***,** the CCPA should use its Section 18(2)(l) power to issue a standardised self-audit protocol specifying, for each of the thirteen categories, what must be tested, across which user segments, and what documentation screenshots, A/B-test logs, consent-flow recordings must be retained and produced on demand. This converts 'self-audit conducted; platform free from dark patterns' from an unfalsifiable assertion into a checkable record. *Second***,** platforms above a defined threshold of reach measured, as the DSA measures very-large-platform status, by monthly active users or transaction value should be required to commission an independent third-party audit on the Flipkart-Myntra-Walmart model already voluntarily adopted by a minority, rather than an internal review. *Third***,** the CCPA should deploy the investigative powers it already holds under Sections 16, 19 and 22 on a risk-based and random basis specifically against filed declarations, treating a compliance letter as an assertion inviting scrutiny rather than a closing document much as a tax return invites, rather than forecloses, assessment. *Fourth***,** and most important, a materially false or knowingly incomplete declaration should itself be treated, on investigation, as a false or misleading representation for the purposes of Sections 21 and 89, so that certifying falsely carries a distinct cost rather than leaving the CCPA to prosecute only the underlying violation, as though no declaration had been made.

The National Consumer Helpline, which recorded 308 dark-pattern complaints between December 2023 and March 2026, should be wired formally into this sequence as a trigger: a threshold volume of verified complaints against a self-certified platform should mandate an independent audit, not merely a further notice.[41] Proportionality matters throughout a small direct-to-consumer seller does not need a Deloitte audit, and requiring one would load compliance costs disproportionately onto smaller players while leaving the largest platforms, best placed to absorb such costs, no worse off. A risk-tiered model concentrates independent verification precisely where the stakes, and the capacity to bear its cost, are both highest.

VII. Conclusion: Self-Audit as a Tool, Not a Substitute for Enforcement

The question with which this essay opened whether an entity better informed than its regulator, but financially incentivised to manipulate the very consumers it audits itself for, can be trusted to self-certify without independent verification has, on eighteen months of Indian experience, a fairly clear answer: not yet, and not without more. The June 2025 advisory was not a retreat

[41] Outlook Business (n 32).

from regulation; it was a rational, resource-constrained response to a genuine problem of scale and hidden information. But a response calibrated to the regulator's constraints is not automatically calibrated to the consumer's protection. Where the two diverge where twenty-six clean declarations coexist with independent findings that most of those platforms still deploy the very practices they declared absent the gap has so far been filled not by platform goodwill but by whichever outside party happened to look: a citizen-audit initiative, an RTI applicant, occasionally the CCPA itself once a fresh complaint arrived.

This is not an argument for abandoning self-audit, which remains the only administratively feasible first line of defence at India's scale. It is an argument against letting it become the last line. Consumer protection is not being abolished by self-certification; it is being quietly relocated from a regulator with statutory powers of investigation and penalty to platforms whose commercial success depends on the very design choices under review. The correction required is not categorical distrust of self-audit, but the deliberate construction of the independent verification that alone converts a platform's account of itself into evidence a regulator, and a consumer, can actually rely upon.