



INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 5 | 2026

Art. 08

When the Price Knows You: The Missing Indian Legal Framework for Personalised Pricing in Digital Marketplaces

Saksham Bharadwaj

Law Student, BBA.LL.B., 4th Year,

Himachal Pradesh National Law University, Shimla

Recommended Citation

Saksham Bhardwaj, *When the Price Knows You: The Missing Indian Legal Framework for Personalised Pricing in Digital Marketplaces*, 5 IJHRLR 81-93 (2026).

Available at www.ijhrlr.in/current-issues/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto & Co. administrator.

For more information,
please contact submission.ijhrlr@gmail.com

When the Price Knows You: The Missing Indian Legal Framework for Personalised Pricing in Digital Marketplaces

ABSTRACT

Digital marketplaces can increasingly tailor prices or commercial offers using location, browsing history, purchase history, device signals and other behavioural data. This creates a legal problem distinct from ordinary dynamic pricing. A price that changes because aggregate demand changes is familiar; a price that changes because a platform predicts that a particular consumer is willing or able to pay more raises questions of transparency, privacy, autonomy, discrimination and market power. India has no dedicated rule requiring a digital seller to disclose that a price has been personalised through automated decision-making. The Consumer Protection Act, 2019, the Consumer Protection (E-Commerce) Rules, 2020, the Guidelines for Prevention and Regulation of Dark Patterns, 2023, the Competition Act, 2002 and the Digital Personal Data Protection Act, 2023 provide partial protection, but they regulate different parts of the problem. This article examines whether the existing Indian framework adequately addresses personalised pricing. It uses doctrinal research supported by regulatory reports, international comparative material and empirical studies on consumer responses. It finds that the principal gap is the absence of a clear, ex ante transparency duty and an auditable framework for establishing when personal data materially influences price. The European Union's express disclosure rule provides a useful model, while the United States' recent surveillance-pricing inquiry demonstrates the need for regulatory visibility into pricing technologies. The article recommends a proportionate Indian regime based on disclosure, data-purpose specificity, algorithmic record-keeping, risk-based auditing, protection against discriminatory variables and accessible redress. The objective is not to prohibit legitimate dynamic pricing, but to prevent opaque data - driven price discrimination.

KEYWORDS

Algorithmic pricing, Consumer protection, Digital marketplaces, Personalised pricing, Privacy.

INTRODUCTION

Price discrimination is not new. Airlines, hotels and retailers have long varied prices according to demand, inventory, timing and customer segments. What is changing is the granularity at which commercial decisions can be made. A digital marketplace can observe browsing and purchasing behaviour, infer characteristics, and combine those signals with real-time market information.

The distinction between dynamic pricing and personalised pricing is legally important. Dynamic or real-time pricing changes prices in response to market conditions without necessarily using information about a particular person. Personalised pricing uses consumer-specific information or profiling to determine what a particular consumer is shown or charged. The European Union expressly recognises this distinction and requires consumers to be informed when a price has been personalised through automated decision-making.¹

The issue deserves attention in India because digital commerce operates through data - rich intermediaries. The Competition Commission of India's e-commerce market study involved 16 platforms, 164 business entities and seven payment-system providers and identified information asymmetry and platform-related competition concerns.² In 2024, the United States Federal Trade Commission began studying "surveillance pricing"; its initial findings indicated that intermediaries may use information including location, browsing history and shopping-cart behaviour in targeted pricing.³

This does not establish that Indian platforms routinely charge different individuals' different prices. The more precise legal question is whether Indian law is sufficiently equipped to detect, disclose and remedy such conduct if it occurs. The question is timely because India has developed rules against dark patterns and, through the Digital Personal Data Protection Act, 2023 and the 2025 Rules, a structured framework for personal-data

¹ Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019, recital 45 and art. 6(1)(ea), available at: <https://eur-lex.europa.eu> (Last visited on 11 August 2026).

² Competition Commission of India, Market Study on E-Commerce in India: Key Findings and Observations (2020), available at: <https://www.cci.gov.in> (Last visited on 11 August 2026).

³ Federal Trade Commission, "FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices" (2025), available at: <https://www.ftc.gov> (Last visited on 11 August 2026).

processing.⁴

The research gap lies at the intersection of consumer law, privacy law, competition law and behavioral economics. Existing Indian regulation addresses misleading pricing, unfair trade practices, data processing and anti-competitive conduct separately, but none provides a dedicated rule for personalised price formation. This article argues that the gap can be addressed without banning personalization. A disclosure-and-accountability model can better balance innovation, commercial freedom and consumer autonomy.

LITERATURE REVIEW

The literature on personalised pricing generally considers economic efficiency, consumer perceptions of fairness, and the ability of privacy or consumer-protection law to constrain the practice. The OECD describes personalised pricing as a form of price discrimination supported by personal data and digital tools and distinguishes it from conventional dynamic pricing.⁵

Empirical work indicates that disclosure alone may not solve the problem. An OECD laboratory experiment in Ireland and Chile found that disclosures had limited effects on consumers' ability to identify and understand personalised pricing, while participants generally considered the practice unfair.⁶ A 2025 FTC staff perspective similarly showed the breadth of personal and behavioral information that may be used in surveillance-pricing systems.⁷

Indian policy has more visibly focused on dark patterns, misleading advertisements, privacy and platform competition. The CCPA's 2023 guidelines identify 13 dark patterns, including bait and switch

⁴ Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025 (notified 14 November 2025), available at: <https://www.meity.gov.in> (Last visited on 11 August 2026); Department of Consumer Affairs, Guidelines for Prevention and Regulation of Dark Patterns, 2023, available at: <https://consumeraffairs.nic.in> (Last visited on 11 August 2026).

⁵ OECD, Personalised Pricing in the Digital Era, OECD Roundtables on Competition Policy Papers No. 222 (2018), available at: <https://www.oecd.org> (Last visited on 11 August 2026).

⁶ OECD, The Effects of Online Disclosure about Personalised Pricing on Consumers, OECD Digital Economy Papers No. 303 (2021), available at: <https://www.oecd.org> (Last visited on 11 August 2026).

⁷ Federal Trade Commission, "FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices" (2025), available at: <https://www.ftc.gov> (Last visited on 11 August 2026).

and drip pricing.⁸ These measures are valuable, but personalised pricing can occur without deceptive interface design: the consumer may see a perfectly clear price that is simply different because the pricing engine has inferred a different willingness to pay.

The present study therefore treats personalised pricing as a distinct regulatory problem. Its contribution is to map the overlap and gaps between consumer law, data protection and competition law and develop a targeted regulatory response.

RESEARCH METHODOLOGY

This study adopts doctrinal and comparative legal research. Primary materials include the Consumer Protection Act, 2019, the Consumer Protection (E-Commerce) Rules, 2020, the Guidelines for Prevention and Regulation of Dark Patterns, 2023, the Competition Act, 2002 and the Digital Personal Data Protection Act, 2023 with the 2025 Rules. Judicial decisions are used to identify broader principles of privacy and autonomy rather than to suggest that Indian courts have already adjudicated personalised pricing as a distinct cause of action.

Secondary and empirical materials include the CCI's e-commerce market study, OECD research and recent FTC material. The international comparison focuses on the European Union because Directive (EU) 2019/2161 expressly requires disclosure where a price is personalised through automated decision-making.⁹

The scope is limited to consumer-facing digital marketplaces and excludes business-to-business pricing and dynamic pricing that does not use individual profiling. A key limitation is the absence of a public Indian dataset establishing the prevalence or magnitude of personalised pricing. The study is therefore preventive: it asks whether Indian law is ready for a practice that technology makes increasingly feasible.

⁸ Central Consumer Protection Authority, Guidelines for Prevention and Regulation of Dark Patterns, 2023, Gazette Notification dated 30 November 2023, available at: <https://consumeraffairs.nic.in> (Last visited on 11 August 2026).

⁹ Directive (EU) 2019/2161, *supra* note 1; see also European Commission, Guidance on the interpretation and application of Directive 2005/29/EC, including personalised pricing, available at: <https://eur-lex.europa.eu> (Last visited on 11 August 2026).

DISCUSSION AND ANALYSIS

1. *The legal problem*

Personalised pricing means using consumer-specific information to influence the price or economic terms presented to a particular consumer or category. Relevant information may include location, purchase history, browsing behaviour, device information, loyalty status or inferred willingness to pay. If Consumer A and Consumer B search for the same product simultaneously but receive different prices because the platform has profiled their likely willingness to pay, the practice is personalised pricing. If the difference results only from inventory or aggregate demand, it is dynamic pricing. Differential pricing is not inherently unlawful. Discounts and segmentation can improve access. The concern arises when the consumer cannot know that profiling affected the price, cannot contest the inference, or is charged more because of sensitive or proxy characteristics. Personalised pricing can turn informational asymmetry into economic asymmetry.

2. *Consumer Protection Act, 2019*

The Consumer Protection Act, 2019 already prohibits several unfair trade practices. Section 2(47) includes materially misleading representations concerning price and other unfair or deceptive practices.¹⁰ Section 18 empowers the CCPA to protect consumer rights and prevent unfair trade practices, while section 94 specifically contemplates measures to prevent unfair trade practices in e-commerce.¹¹

These provisions could address personalised pricing accompanied by deception—for example, where a platform falsely presents a personalised price as a universally available discount. The difficulty is that an individually generated price may be technically accurate while remaining opaque. A platform can truthfully display ₹1,200 without revealing that it assessed the consumer's purchasing power.

The 2023 dark-pattern guidelines strengthen the framework. They define dark patterns as deceptive designs that impair consumer autonomy and identify 13 specified practices.¹² The government

¹⁰ Consumer Protection Act, 2019, s. 2(47), available at:

<https://www.indiacode.nic.in> (Last visited on 11 August 2026).

¹¹ Consumer Protection Act, 2019, ss. 18, 21 and 94, available at:

<https://www.indiacode.nic.in> (Last visited on 11 August 2026).

¹² Central Consumer Protection Authority, Guidelines for Prevention and

has subsequently encouraged e-commerce platforms to self-audit.¹³ Yet personalised pricing may fall outside classic dark patterns because the manipulation occurs in the pricing engine rather than the interface.

The Consumer Protection (E-Commerce) Rules, 2020 are more directly relevant. They apply to digital commerce and prohibit price manipulation intended to gain unreasonable profit through unjustified pricing; they also prohibit discrimination between consumers of the same class or arbitrary classification affecting rights.¹⁴ These provisions provide a foundation, but leave difficult questions: how does a consumer prove personalisation, what is an arbitrary classification, and when does data-based segmentation become unjustified discrimination? The rules contain the beginnings of a substantive prohibition but no clear procedural right to know whether personalisation occurred.

3. Data protection: regulating the input, not the output

The DPDP Act is relevant because personalised pricing may depend on personal data. Section 4 permits processing for a lawful purpose where consent has been obtained or a legitimate use applies, while section 5 requires notice identifying the data and purpose of processing.¹⁵ Sections 11–13 provide rights concerning access, correction, erasure and grievance redressal.¹⁶

The key issue is purpose specificity. A marketplace saying that browsing history will be used to "personalise your experience" may not tell the consumer that the information can materially affect the price. A compliant data notice should not become a back door for economically consequential profiling that consumers never meaningfully understand.

The DPDP framework is not itself a pricing-fairness law. It regulates personal-data processing, not the fairness of the resulting price. A platform may lawfully process data while creating a consumer-protection concern through an exploitative

Regulation of Dark Patterns, 2023, *supra* note 8.

¹³ Department of Consumer Affairs, "CCPA Advisory on Self-Audit by E-Commerce Platforms for Detecting Dark Patterns" (5 June 2025), available at: <https://consumeraffairs.nic.in> (Last visited on 11 August 2026).

¹⁴ Consumer Protection (E-Commerce) Rules, 2020, rr. 4 and 5, available at: <https://consumeraffairs.nic.in> (Last visited on 11 August 2026).

¹⁵ Digital Personal Data Protection Act, 2023, ss. 4–5, available at: <https://www.indiacode.nic.in> (Last visited on 11 August 2026).

¹⁶ Digital Personal Data Protection Act, 2023, ss. 11–13, available at: <https://www.indiacode.nic.in> (Last visited on 11 August 2026).

price; conversely, a price may be unfair even where the underlying processing is lawful. The inquiries must remain distinct. MeitY notified the Digital Personal Data Protection Rules, 2025 on 14 November 2025.¹⁷ This creates a stronger institutional base for addressing data-driven commercial practices, but it does not remove the need for a pricing-specific rule.

4. Privacy and informational autonomy

The Supreme Court's recognition of privacy as a fundamental right in *K.S. Puttaswamy v. Union of India* is relevant because informational privacy concerns control over personal information and its uses.¹⁸ Personalised pricing raises a related concern: consumers may lose economic autonomy when data is silently converted into a prediction of willingness to pay.

The constitutional proportionality framework should not be mechanically applied to every private transaction. However, its principles of legality, legitimate purpose and proportionality provide a useful normative benchmark for data-intensive commercial practices. The stronger the economic consequence of profiling, the stronger the case for transparent notice and safeguards.

5. Competition Law

Competition law adds a market-power dimension. Section 4 of the Competition Act, 2002 addresses abuse of dominant position, including specified forms of discriminatory or unfair pricing.¹⁹ Personalised pricing by a non-dominant firm will not attract section 4 merely because consumers receive different prices. But where a dominant platform uses extensive data advantages to impose exploitative or discriminatory conditions, personalised pricing may become relevant.

The CCI's e-commerce study identified information asymmetry and data advantages as important competition concerns.²⁰ The competition question is therefore also whether a platform's control over data gives it an advantage competitors cannot replicate or audit.

¹⁷ Ministry of Electronics and Information Technology, Digital Personal Data Protection Rules, 2025, *supra* note 4.

¹⁸ *K. S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

¹⁹ Competition Act, 2002, s. 4(2)(a)(ii), available at: <https://www.indiacode.nic.in> (Last visited on 11 August 2026).

²⁰ Competition Commission of India, Market Study on E-Commerce in India: Key Findings and Observations (2020), *supra* note 2.

Personalised pricing can consequently fall between consumer and competition regulators, making coordination important.

6. *European Union*

The EU provides the clearest legislative benchmark. Directive (EU) 2019/2161 requires traders, where applicable, to inform consumers that a price has been personalised on the basis of automated decision-making. It deliberately distinguishes this from dynamic or real-time pricing responding to market demand without individual profiling.²¹

The model does not prohibit personalisation or require disclosure of source code. It creates a transparency trigger at the point of purchase. This protects trade secrets while addressing the information asymmetry. The rule operates alongside the GDPR, including its provisions on automated decision-making and profiling.²²

For India, the EU approach is attractive because it is proportionate and technologically neutral: disclosure is triggered by the use of personalised pricing rather than by a particular algorithm.

7. *United States*

The United States illustrates a regulatory-investigation pathway. In July 2024, the FTC ordered eight companies to provide information about surveillance-pricing products using personal and behavioural data.²³ Its subsequent findings indicated that location, demographics, browsing patterns, shopping history, mouse movements and abandoned carts could be relevant inputs.²⁴

The lesson for India is methodological. Before legislating broadly, regulators can study the technology, intermediary market and actual prevalence. CCPA-CCI cooperation, information requests and controlled audits could establish an Indian evidence base.

8. *Empirical evidence and the limits of disclosure*

The OECD experiment complicates a simple "just disclose it"

²¹ Directive (EU) 2019/2161, *supra* note 1.

²² Regulation (EU) 2016/679 (General Data Protection Regulation), art. 22, available at: <https://eur-lex.europa.eu> (Last visited on 11 August 2026).

²³ Federal Trade Commission, "FTC Issues Orders to Eight Companies Seeking Information on Surveillance Pricing" (23 July 2024), available at: <https://www.ftc.gov> (Last visited on 11 August 2026). ²⁴Federal Trade Commission, *supra* note 3.

²⁴ *Ibid.*

solution. Disclosures had limited effects on consumers' ability to identify and understand personalised pricing, although participants generally considered it unfair.²⁵ A disclosure must therefore be prominent and standardised, not buried in a privacy policy.

A practical rule could require a short notice at the point of price presentation: "This price has been personalised using automated analysis of information associated with your account." A link could explain the broad categories of data used and whether personalisation can increase, decrease or both increase and decrease the price.

9. Why a blanket ban is premature?

An outright ban could remove beneficial forms of segmentation, including student discounts, loyalty rewards and targeted discounts. A price-sensitive consumer may receive a lower price because the system predicts abandonment.

The better distinction is between legitimate personalised offers and opaque or harmful personalised prices. Relevant factors should include the use of sensitive or proxy characteristics, the magnitude of the difference, quality of disclosure, ability to contest, market power and targeting of vulnerable consumers.

10. Evidentiary gap

The central practical weakness is proof. A consumer sees only the final price; the algorithm's inputs, experiments, alternative prices and audit logs remain with the platform. Without access to records, the consumer cannot easily establish differential treatment.

This creates a proof asymmetry: the party most capable of proving personalisation controls the evidence. A future framework should therefore require risk-based record keeping for significant personalised-pricing systems. Records need not reveal source code. They should preserve the categories of data used, the pricing decision class, relevant price ranges and material model changes for a defined period.

²⁵ OECD, The Effects of Online Disclosure about Personalised Pricing on Consumers, *supra* note 6.

FINDINGS

The study produces five findings. First, personalised pricing is legally distinguishable from ordinary dynamic pricing. Second, Indian consumer law can address deceptive or arbitrary pricing but does not clearly create a point-of-sale disclosure duty. Third, the DPDP framework regulates data processing but does not determine whether a resulting price is fair. Fourth, competition law becomes relevant where pricing is connected to dominance or data advantages, but is not a complete consumer remedy. Fifth, the central problem is proof because consumers cannot ordinarily observe the counterfactual price they would have received without profiling.

The absence of a public Indian dataset proving widespread personalised pricing is also significant. Regulation should therefore be evidence-based, beginning with transparency, regulator access and controlled monitoring.

RECOMMENDATIONS

1. **Express disclosure duty:** Amend the Consumer Protection (E-Commerce) Rules to require clear point-of-price disclosure whenever automated decision-making materially personalises a price.
2. **Dynamic/personalised distinction:** Do not impose the same duty on demand - based dynamic pricing where no consumer-specific profiling is used.
3. **Specific data-purpose disclosure:** Where personal data is used for pricing, the notice should expressly identify pricing or willingness-to-pay assessment as a purpose. Generic "personalised experience" language should not suffice.
4. **Risk-based audit trail:** Large marketplaces using personalised pricing should retain records of relevant data categories, pricing rules, material model changes and price ranges, while protecting trade secrets.
5. **High-risk variables:** Regulators should identify protected characteristics and close proxies whose use in price formation is prohibited or presumptively high-risk, subject to lawful exceptions.
6. **Consumer contestability:** Consumers should have a simple mechanism to ask whether a price was personalised and request review of a material adverse difference. No source-code

disclosure should be required.

7. **CCPA-CCI coordination:** Consumer cases involving market power or data advantages should be capable of referral to the CCI, and consumer-facing deception should be referable to the CCPA.
8. **Market studies:** Regulators should conduct controlled studies across travel, retail, food delivery, mobility and digital services before imposing broad restrictions.
9. **Standardised notice:** A short uniform statement or icon should appear before payment rather than only in a privacy policy.
10. **Proportionate remedies:** Remedies should include refund of provable excess payment, compensation, corrective disclosure, restriction of improperly used data and penalties for repeated or systemic violations.

CONCLUSION

Personalised pricing changes the relationship between consumer data and market price. The concern is not that technology allows firms to change prices, but that the same data infrastructure used to predict what a consumer will click may predict what that consumer will pay.

India does not start from a regulatory vacuum. Consumer law, e-commerce rules and dark-pattern guidelines provide tools against unfair conduct; the DPDP framework governs personal-data processing; and competition law can address conduct linked to market power. Yet these instruments do not give a simple answer to the question: "Was this price calculated differently because the platform knew something about me?"

The EU demonstrates that an express disclosure duty can protect transparency without banning personalisation or requiring algorithmic disclosure. The US demonstrates the value of regulatory investigation into the intermediaries behind surveillance pricing. India should combine both lessons: transparency at the consumer interface with deeper regulatory visibility behind it.

The appropriate response is targeted rather than prohibitory. India should distinguish dynamic from personalised pricing, require meaningful disclosure, restrict high-risk variables, preserve auditable records, enable contestability and coordinate consumer and competition regulators. Clarifying these rules now would allow legitimate innovation while reducing the risk that personal data becomes

an invisible tax on consumers.

RESEARCH NOTE

This article is based on primary legislation, regulatory materials, judicial authority, international regulatory material and empirical research. The study does not assert that personalised pricing is widespread in India; the absence of a public Indian prevalence dataset is expressly identified as a limitation.