AI-POWERED PERSONALIZATION IN ONLINE SHOPPING: NAVIGATING INDIA'S CONSTITUTIONAL PRIVACY AND CONSUMER PROTECTION FRONTIERS

Dr. Koneru Anuradha, Associate Professor, Smt. V. D. Siddhartha School of Law, Siddharth Academy of Higher Education, Deemed to be University, Vijayawada.

ABSTRACT

The fast adoption of personalization that is facilitated by artificial intelligence (AI) in online shopping has significantly redefined the digital commerce environment in India because it has altered the experiences of consumers, the way business is conducted in the market, and the governance of data over the Internet. Although algorithmic personalization promotes the efficiency, convenience, consumer engagement, and advertising with the help of the predictive analytics and recommendations, it also brings to the fore significant constitutional and regulatory issues that concern the informational privacy, the autonomy, the transparency, and consumer welfare. This paper is a critical analysis of AI-enhanced personalization within the constitutional framework of India, especially the right to privacy expressed in the Constitution, Article 21 as interpreted by Justice K.S. Puttaswamy. Union of India, together with new legal safeguards provided by the Digital Personal Data Protection Act, 2023 and the Consumer Protection Act, 2019. This paper will examine how personalized pricing and behavioral targeting, as well as automated decision making, can result in results of discrimination, information asymmetry, and control over consumer choice, thus altering the agreed-upon principles of fairness, consent, and accountability. It also measures how suitable the consumer protection framework in India is to deal with the problems of algorithmic opaqueness and data-driven exploitation, in comparison with regulatory models in other countries. This article advocates a moderate regulatory system that would strike a balance between technological innovation and constitutional morality and consumer rights through the use of a doctrinal and analytical approach. The paper ends with a set of legal and policy recommendations that could be put in place to enhance transparency, algorithmic responsibility, and data fiduciary responsibility to make sure that AI-based personalization of online markets does not contradict the constitutional principles of India and consumer protection goals.

Keywords: Artificial Intelligence (AI); Online Shopping; Algorithmic Personalization; Right to Privacy; Digital Personal Data Protection Act, 2023; Consumer Protection Act, 2019; Informational Self-Determination; Algorithmic Transparency; Consumer Autonomy; Data Governance in India.

Introduction

The boom of electronic commerce in India has been inseparably connected to the quick development and implementation of the artificial intelligence (AI) technologies that have radically changed the experience of consumers in the digital marketplaces. Due to the AI-informed systems, the operational architecture of the e-commerce platform is now heavily reliant on AI, with businesses being able to process large amounts of consumer data in real-time and use advanced technologies to provide algorithmic recommendations, personalised ads, dynamic pricing models, and predictive consumer analytics. Indeed, the innovations have made the shopping experience more efficient, convenient, and engaging by providing customized shopping experiences that adapt to personal preferences, behavioural tendencies, and buying behaviour.[1] Nevertheless, the growing use of AI-enhanced personalization also poses essential legal and constitutional issues, especially regarding the issue of data security, information privacy, and consumer control in the context of the developing Indian online economy. The fundamental principle of AI-based personalization is the massive accumulation, computing, and analysis of personal data and sensitive behavioural and transactional information. E-commerce sites regularly collect data items, including browsing history, location data, frequency of purchase, and even a machine-learned inference of preferences. Although this type of data-driven personalization has a justifiable rationale in terms of the enhancement of consumer satisfaction and competitiveness in the market, it has also brought about an unequal distribution of power between digital platforms and consumers.[2] This asymmetry is further enhanced by the black box aspect of algorithmic decision-making where consumers are often not aware of how their data is gathered, processed, or sold to them, thus, compromising meaningful consent and choice.

The constitutional view of the application of AI technologies in e-commerce should be considered in the background of the Constitution of India, Article 21, which affirms the privacy of personal liberty and life. In the landmark decision known as Justice K.S. Puttaswamy (Retd.) v. Union of India,[3] the supreme court made it categorical that the right to privacy is inherent to Article 21, and the privacy of information was also included in the right to privacy, and so was

[1] Ajay Bhushan Pandey, *Artificial Intelligence and Digital Economy in India* (2020) 62 *Journal of the Indian Law Institute* 45.
[2] Shubha Ghosh, 'Data, Algorithms and Consumer Exploitation in Digital Markets' (2021) 6 *Indian Journal of Law and Technology* 112.
[3] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

the fact that an individual had control over personal information. The Court highlighted that any breach of privacy should meet the legality, necessity and proportionality tests, thus subjecting the State and non-State actors in the process of data processing to substantive restrictions. Within the e-commerce setting, a parallel responsibility of this constitutional mandate is on the private digital platforms with the consumption of which AI-based data practices will not lead to arbitrary, excessive, or disproportionate encroachment on consumer privacy. Article 21 is more relevant in the digital marketplace where AI systems constantly follow and shape consumer behaviour. Individual pricing systems, such as, can lead to discriminatory effects whereby various prices are passed to consumers based on algorithmic profiling, of which the issue of justice and equality is of concern.[4] Likewise, targeted advertising and recommendation engines can also influence consumer decision-making by using cognitive biases to undermine personal free will and autonomy. These practices are technologically savvy and they threaten to violate the constitutional ethos of dignity and individual liberty that forms the basis of the right to privacy in India.

Besides the constitutional protection, the Consumer Protection Act, 2019 (CPA) also represents a major intervention in the statutory form, which seeks to deal with unfair trade practices and safeguard consumer interests in the digital era.[5] The CPA also applies to the e-commerce organizations and specifically aims at avoiding such practices that are pursued misleadingly, exploiting or being detrimental to the consumers. The Consumer Protection (E-Commerce) Rules, 2020, which are based on the Act, also present the online platforms with a duty of maintaining transparency and information disclosure and fair treatment of consumers. The latter provisions especially apply to the regulation of AI-based personalization, making the algorithmic opacities, as well as the manipulation with the use of data, potentially unfair trade practices in accordance with the Act. Another issue arises, though, when it comes to the potential conflict between the commercial needs of companies to use AI technologies to create even greater personalization and the legal requirements concerning the protection of the rights of the consumers. Even though AI is beneficial to businesses by helping them to maximize user interaction and revenues, its unregulated application could spell out exploitative data usage that contravenes the justices of fairness, affirmation, and responsibility as enshrined in the consumer law.[6] The CPA which is read together with constitutional privacy jurisprudence

[4] Pratiksha Baxi, 'Algorithmic Discrimination and Equality in Digital Markets' (2022) 4 *NUJS Law Review* 233.
[5] Consumer Protection Act, 2019, ss 2(47), 49.
[6] Avinash Kumar, 'Unfair Trade Practices in E-Commerce: An Indian Perspective' (2021) 63 *Journal of the Indian Law Institute* 389.

implicitly requires that practice of personalization should be transparent, non discriminatory and that it should not violate consumer autonomy. A lack of compliance with these standards can lead to the e-commerce organisations being exposed to regulatory risks and liabilities of performing unfair or deceptive acts.

Moreover, the changing regulatory environment in India is an indicator of the growing appreciation of the necessity to balance technological innovation with constitutional and consumer protection standards. The Digital Personal Data Protection Act, 2023, which strengthens the fiduciary duty of data processors and focuses on purpose restriction, data reduction, and informed consent.[7] Though it is mostly a data protection legislation, its tenets have direct bearing on AI-based personalization in e-commerce since limits in the scope of use of consumer data in algorithmic profiling and monetary benefit are restricted. Collectively, both the constitutional jurisprudence and consumer protection law presuppose a paradigm shift in the domain of the governance of the digital commerce towards the rights-based approach.

Overall, although AI-based personalization has helped revolutionize online shopping because it makes it more efficient and immersive, it has also emerged as a complicated issue on the junction of constitutional privacy and consumer protection law in India. Without a regulated perspective on the unchecked use of AI technologies, informational self-determination and consumer autonomy is under a threat hence there is a need to have a balanced regulatory framework that balances innovation and constitutional morality. An upright amalgamation of Article 21 safeguard with the Consumer Protection Act requirement of unfair practices is necessary to ascertain that AI-based e-commerce develops in a way that is technologically progressive and arguably legal.

Constitutional Constraints on E-Commerce Platforms: Privacy, Equality, and Freedom of Trade

The Indian constitutional system is very instrumental in governing the fast-growing sphere of e-commerce, especially when it comes to utilizing the data-driven and AI-supported business models. The jury of rights that are established in the Constitution was developed long before the emergence of digital marketplaces, but it has been dynamic to respond to the modern challenge of technology. E-commerce companies (ECS) are a potent non-State actor that is

[7] Digital Personal Data Protection Act, 2023, ss 4–8.

becoming more and more demanded to strategize their business models in line with the constitutionally established rights, particularly those rights concerning privacy, equality, and freedom of trade. These rights do not work in a vacuum but as interdependent limitations that define the acceptable scope of AI personalization and data analysis within the context of online shopping. The Supreme Court has acknowledged that the right to privacy is a fundamental right as stated in Article 21 of the Constitution when it decided in favor of the plaintiff in Justice K.S. Puttaswamy (Retd.) v. Union of India[8] was a landmark case in the Indian constitutional law. The Court believed that privacy inherently belongs to life and individual liberty and entails informational self-determination, decisional autonomy, and safeguarding of personal information. Notably, the ruling stipulated that any encroachment into privacy has to meet a three-fold test of legality, necessity and proportionality. This proportionality rule has a profound effect on e-commerce websites, which regularly collect and process the consumer data at a large scale to power the AI-based personalization algorithms.

The necessity principle under the constitutionally accepted rules and regulations of ECS requires the ECS to have a legitimate and clearly defined purpose of collection and processing of personal data.[9] Over-data gathering, the behavioural profiling more than the expectation of the consumer or retention of data without determining its purpose, is something that might not comply with this constitutional standard of the algorithmic experiment. The AI systems based on the constant monitoring of consumer behaviour, thus, need to be structured in such a way that they do not violate the principles of data minimization and the limitation of purpose. In this respect, the Puttaswamy doctrine indirectly assigns the data fiduciary-type duties to the private digital platforms, although they are not conventional actors of the State. Additionally, the proportionality requirement insists on some kind of balance between the interests of the business and the rights of the individual. Personalization can be used to increase consumer convenience; however, intrusive consumer privacy and autonomy can be violated by hyper-targeted advertising, predictive pricing, and psychological profiling disproportionately.[10] This could end up turning consumers into passive data subjects instead of free market agents, and thus eroding the dignity-based understanding of privacy promoted by the Supreme Court. Therefore, the constitutional privacy jurisprudence is a substantive limitation governing how

---

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

[9] Apar Gupta, 'Privacy and the Constitutional Limits of Data Collection in India' (2019) 61 *Journal of the Indian Law Institute* 34.

[10] Arghya Sengupta & Vidhi Centre for Legal Policy, *Privacy, Proportionality and the Digital Economy* (2018) 57.

the AI technologies can be used in e-commerce ecosystems.

Along with privacy, Article 14 of the Constitution which proclaims equality before the law, and forbids arbitrariness, takes on a new meaning in the light of the work of algorithms. The Supreme Court has always applied Article 14 as the protection of arbitrary, unreasonable, and discriminative State action.[11] Though e-commerce players are privately operated organizations, their growing dominance of online marketplaces and access to consumers is making their behaviours quasi-public by default. Algorithms used to suggest recommendations and personalized pricing models utilized by ECS can be unconsciously biased or discriminatory due to the use of distorted sets of data or unclear machine-learning decisions. As an example, AI-based personalization can lead to unequal treatment of consumers on the basis of the attributes proposed by AI, namely, gender, location, income level, or purchasing power.[12] This preferential treatment without transparency or reasonable explanation can turn into digital arbitrariness and can destroy the egalitarian spirit of Article 14. Algorithms profiling in price discrimination, a specific example, is a source of concern to equity and equal opportunities to goods and services in the Internet market. Although it is not unconstitutional in itself, the non-transparency and non-accountability of the process of differential pricing by means of AI systems can be incompatible with the constitutional principle of non-arbitrariness.

Also, the issue of algorithmic bias presents a structural problem to equality by incorporating historic biases into automated systems. When learning AI models are trained on datasets that portray the current socio-economic inequalities, they would support exclusionary results instead of substantive equality.[13] In this respect, Article 14 acts as a normative reference point in the evaluation of the fairness of AI-related e-commerce activities. Arbitrariness is therefore ruled out by the constitution even in cases of formal equality and requires to be accountable, explainable, and fair in algorithmic governance. The constitutional basis of the operation of e-commerce enterprises in India is article 19 (1)(g) of the Constitution which guarantees the freedom of practising any profession or of carrying on any occupation, trade or business. This liberty allows ECS to be creative, use new technologies, and practice competitive market dynamics such as using AI to personalize and address consumers. This right is however not

[11] *E.P. Royappa v. State of Tamil Nadu*, (1974) 4 SCC 3

[12] Anupam Chander, 'The Racist Algorithm?' (2017) 115 *Michigan Law Review* 1023.

[13] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 *International Data Privacy Law* 76.

absolute and it is clearly subject to reasonable limitations to the interest of the general population under Article 19(6).

Consumer protection is a justifiable reason to introduce such reasonably sensible restrictions upon commercial liberties.[14] The State has the constitutional authority to control trade and business behaviors that are injurious to consumer welfare, manipulatory of market fairness, or that are degradatory of the individual rights. Within the framework of AI-based e-commerce, ethical limitations that would help avert unfair trade practices, personalization that is misleading and abusive use of data are well within the constitutional reach. Therefore, even though ECS have the freedom to operate business, they need to do so in such a way that do not infringe consumer rights and constitutional values. Article 19(1)(g) in interaction with Articles 14 and 21 highlights the necessity of the balanced nature of AI-driven personalization regulation. Anonymity, equality, and autonomy of a consumer cannot be sacrificed in the name of commercial innovation. The market order that is depicted in the Constitution is non-only efficient and just, but also fair and respectful of rights.[15] Constitutional restrictions, in this respect, do not choke the e-commerce growth, but offer a normative guideline that guarantees sustainable and ethical online business.

Conclusively, rights that are established under the constitution act as the much needed protection under the fast changing e-commerce environment in India. Articles 21, 14 and 19(1)(g) ensure privacy, equality and trade freedom respectively, and limit excessive exploitation of data, arbitrariness of algorithms and discrimination, and allow innovation under conditions of consumer-focused regulations. Collectively, these rights establish a constitutional framework aimed at balancing the development of technology and the protection of basic rights. As AI-powered personalization becomes increasingly pervasive, adherence to constitutional principles will be indispensable in ensuring that digital markets remain fair, transparent, and aligned with India’s constitutional morality.

Statutory Regulation of Digital Commerce: Data Protection, Consumer Welfare, and Intermediary Accountability

The fast-growing e-commerce environment in India functions under a multi-layered statutory framework that aims at controlling the gathering and utilization of personal information and

---

[14] *Chintaman Rao v. State of Madhya Pradesh*, AIR 1951 SC 118.
[15] B.N. Srikrishna, *Framing a Data Protection Framework for India* (Committee Report, 2018) 12–15.

safeguarding the interests of consumers and ensuring that online intermediaries can be held accountable. With AI empowered personalization as a part of online shopping, the role of statutory intervention gains an increased importance in the process of achieving equilibrium between technological innovation and human rights and market justice. Three major legislative tools, such as the Digital Personal Data Protection Act, 2023 (DPDPA), the Consumer Protection Act, 2019 (CPA), and the Information Technology Act, 2000 (IT Act) jointly regulate the legal duties of e-commerce organizations and organize the acceptable boundaries of the data-driven business practices.

The Digital Personal Data Protection Act, 2023 is the most extensive piece of legislation the state of India has ever taken in response to the mass processing of data in the digital economy. The Act acknowledges that personal data protection is a rights-based regime; the regime that is based on the principles of consent, purposes, and accountability.[16] It presents the principle of the so-called data principal and data fiduciary, thus, introducing positive commitments to the institutions that gather and process personal information. Specifically, when it comes to e-commerce, the consent of using consumer data as an input in AI-related personalization, profiling, or targeted advertising, platforms that serve as data fiduciaries must seek free and specific, informed, and unambiguous consent before data is processed. One of the important contributions of the DPDPA is that it provides the description of the fiduciary duties, according to which data processors should behave fairly and reasonably, paying attention to the accuracy of data, security protection, and the mechanisms of grievances.[17] These commitments are specifically applicable through AI-intelligent e-commerce systems based on the continuous data streams to optimize the algorithmic models. The Act limits the random data gathered by ensuring that it is limited to purpose, which minimizes data usage, thus preventing over-surveillance of consumer behaviour. In addition, the liberties to privacy of the information principals, such as the right to information, right to correction, right to erasure, and the right to redress grievances reinforced personal authority of personal data in the digital market places.

Regulatively speaking, the DPDPA supports the constitutional principles of privacy that were established in Justice K.S. Puttaswamy v. Union of India through the act of translating them into binding statutory obligations to be remedied by the private actors.[18] Soft power The

[16] Digital Personal Data Protection Act, 2023, ss 2, 6–8.
[17] Apar Gupta, 'India's New Data Protection Regime: Rights, Duties and Enforcement' (2023) 65 *Journal of the Indian Law Institute* 112.
[18] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

emphasis on consent and fairness restricts the opaque AI practices that compromise consumer autonomy, although the Act does not explicitly regulate automated decision-making. As a result, the DPDPA is a ground breaking law that regulates the personalization of AI in e-commerce by making sure that the innovation will not oppose to the informational self-determination. In addition to data protection regime, the Consumer Protection Act, 2019 is an effective tool of protecting consumer interests in the digital age. The CPA has a broad definition of the term unethical trading practice that involves misleading advertisements, false representations, and misleading business practices.[19] Algorithms of recommendations and targeted advertisements that are used in the environment of AI-based e-commerce to control consumer choice or distort the information on the material may be classified as unfair trading practices. In this manner, the Act will deal with the asymmetry of information and bargaining power of the digital marketplaces.

Notably, the CPA is applied to the entities of online commerce as well and online consumers can be considered a specific category that needs to be more protected. The Act provides the Consumer Protection (E-Commerce) Rules, 2020, with a certain set of requirements to digital platforms, such as information disclosure, price transparency, and forbidden manipulative activity.[20] These regulations are especially applicable in the context of controlling AI-controlled personalization since they aim at making sure that automated systems do not deceive the consumer by using hidden promotions, pricing, or prioritization of products and services. Product liability provisions and enhancements in the enforcement mechanisms by consumer commissions and the Central Consumer Protection Authority (CCPA) are also brought forward by the CPA. This regulatory framework allows the examination of algorithmic business models that are not based on the benefit of consumers. Striking the e-commerce platforms responsible of unfair and misleading practices, the CPA serves as the balancing force that can stem the uncontrolled use of AI technologies in the virtual shopping arena.[21] Therefore, the consumer protection legislature serves as a substantive control over the market power of data-driven platforms.

The amended version of the Information Technology Act, 2000, is the first regulatory effort to control electronic commerce and digital intermediaries in India. Although the Act was not

[19] Consumer Protection Act, 2019, s 2(47).
[20] Consumer Protection (E-Commerce) Rules, 2020, rr 4–6.
[21] Avinash Kumar, 'Regulating E-Commerce under the Consumer Protection Act, 2019' (2021) 63 *Journal of the Indian Law Institute* 389.

initially intended to deal with AI-based personalization, its sections on intermediary liability and due diligence still apply to e-commerce platforms. The IT Act, section 79, offers the intermediaries protection of safe harbour with conditions that the intermediary must comply with the stipulated due diligence.[22] Entities that deal with e-commerce, which provide a third-party content or enable transactions, must become responsible and stop unlawful or harmful activities on the websites. The Rules on Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021 go further to discuss the due diligence of the intermediaries which include grievance redressal, content moderation and transparency.[23] Though mainly intended to control online content, such responsibilities have secondary effects on AI-assisted e-commerce sites, where automation can be held accountable in interfering with relationships between consumers. Lack of due diligence can culminate into loss of safe harbour protection consequently exposing the platforms to legal liability.

Within the framework of an e-commerce process that is run through artificial intelligence, the liability of mediators takes on a more subtle form. Curatorial algorithms, ranking algorithms, and even advertisement-personalization are ceasing to be passive means but aggressive drivers of consumer decision-making. This undermines the classical view of intermediaries as neutral facilitators and demands a reevaluation of accountability standards by the IT Act.[24] Moreover, with the growing mediation of commercial interactions by AI systems, due diligence should be applied to both algorithmic governance and transparency. The combination of the DPDPA, CPA, and IT Act results in a unified regulatory framework of e-commerce platforms that govern it in a variety of points of view-data protection, consumer welfare, and intermediary responsibility. Although each of the statutes has its specific sphere of action, their interaction is to subject the e-commerce players, who use the AI-driven personalization, to multiple layers of obligations. This convergence in regulation is indicative of a wider change in Indian law to rights-based digital regulation.

To sum up, the legal system regulating e-commerce is currently being slowly modified in India to accommodate the challenges posed by the introduction of AI-driven personalization. The Digital Personal Data Protection Act, 2023 provides responsibilities in the processing of data, the Consumer Protection Act, 2019 guarantees the consumer against fraudulent and unfair

---

[22] Information Technology Act, 2000, s 79.
[23] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[24] Shubha Ghosh, 'Intermediary Liability and Algorithmic Accountability in India' (2022) 7 *Indian Journal of Law and Technology* 56.

practices, and the Information Technology Act, 2000 has stipulated the standard of intermediary responsibility and due diligence. Collectively, these laws aim at striking a balance between technological innovation and constitutional values and consumer rights, thereby laying the groundwork for a fair, transparent, and accountable digital marketplace.

Algorithmic Personalization in E-Commerce: Technical Architecture and Associated Legal Risks

The technological infrastructure of the modern e-commerce platform is built on artificial intelligence-based personalization, which defines consumer behavior in the digital market and automated commercial decision-making at scale. The functioning of these personalisation systems is based on complicated algorithmic structures which are grounded on massive data processing, predictive analytics and the constant optimisation of their models. Although these mechanisms create positive effects in terms of efficiency and consumer involvement, they also pose a serious legal and ethical threat to the areas of privacy, equality, transparency, and consumer autonomy. A subtle grasp of the technical mechanisms and its surrounding dangers is hence required with the scope of assessing the legality of the AI-based personalization in online shopping. On the bottom level of AI personalization, there is the data pipeline, which defines the way in which consumer data is gathered, processed, and converted into actionable insights. E-commerce sites regularly receive large amounts of user data, such as demographic details, browsing history, purchase history, location data and device identifiers. This unstructured data is then fed through feature engineering, whereby appropriate attributes are filtered, improved and organized to use in training machine learning models.[25] The role of feature engineering in determining the outcome of the algorithms cannot be overstated because the features determine how the consumer preferences and behaviours are perceived by the AI systems. After that, machine learning algorithms are applied to historical data to discover trends and relationships that may forecast the behavior of future consumers.

This data pipeline is continuous by nature, which enables the personalization systems to become dynamic and adjust their strategy to the current recommendations and pricing in real-time. Nonetheless, this intensive data acquisition and model re-training poses a significant question of data reduction, limitation of purpose, and informed consent. The unnecessary data storage can be much more than is reasonably adequate to service provision, and that is in

[25] Ian Goodfellow, Yoshua Bengio & Aaron Courville, *Deep Learning* (MIT Press 2016) 98.

conflict with the new data protection standards and the constitutional privacy values.[26] In addition to this, many consumers do not have the meaningful awareness of the scope and consequences of such data processing, which leads to the asymmetry and the lack of control over personal data. The most obvious form of AI personalization in e-commerce is in the form of recommendation algorithms. Such systems dictate the kind of products, services or advertisements shown to the consumers thus having a great influence on the purchasing decisions. One of the most widely used methods is collaborative filtering that creates recommendations through the similarity of users or items.[27] Collaborative filtering can be used to forecast individual preferences by examining some patterns of collective behavioural patterns without necessarily asking the consumers to give any explicit preference. This method is further refined by matrix factorisation techniques that break down large sets of interaction data into latent factors of hidden user preferences and item properties.

More recently, the use of deep neural networks and other state of the art machine learning models has become common among e-commerce platforms in an effort to increase the accuracy of the recommendations. These models can handle large datasets containing complex and non-linear relationships in large datasets, and can combine and combine different types of data, including text, images, and behavioural signals.[28] Although these systems enhance the accuracy of personalization, they also enhance the secrecy of algorithms. Deep learning models can be considered a type of black box and therefore, consumers, as well as regulators, can hardly comprehend how certain recommendations are produced and why certain products are prioritised over others. Besides suggestions, AI systems are essential in dynamic pricing methods used by online commercial organizations. Dynamic pricing is the prices which are dynamically adjusted depending on a number of factors, such as user profiles, browsing history, purchasing capacity, geographical location, time of access, and even the type of device used.[29] The goal of AI-based price optimisation models is also to maximise the revenue through predicting willingness to pay by the consumers and modifying prices based on their willingness. Although this could help in improving the efficiency of the market, it creates issues

---

[26] Apar Gupta, 'Data Minimisation and Purpose Limitation under Indian Data Protection Law' (2023) 65 *Journal of the Indian Law Institute* 145.
[27] Jannach, Zanker & Felfernig, 'Recommender Systems: An Introduction' (2011) 25 *Cambridge University Press* 67.
[28] Ricci, Rokach & Shapira, *Recommender Systems Handbook* (Springer 2015) 211.
[29] Ezrachi & Stucke, 'Artificial Intelligence and Collusion: When Computers Inhibit Competition' (2017) 5 *Oxford Journal of Competition Law* 112.

of fairness, discrimination, and transparency.

Individual pricing can lead to the situation when similar consumers can be offered varying prices on the same products or services without their awareness. When this type of differentiation is informed by deduced socio-economic variables or behavioural profiling, it may go beyond the border of acceptable price variation and discrimination pricing.[30] Algorithms pricing under the veil adds to the information asymmetry and lack of trust in information since people cannot determine whether the pricing decisions are justified or not either. The implementation of AI personalization systems brings out various inter-linked risks that could have legal and constitutional ramifications. The risk of privacy breaches is considered to be one of the most striking issues due to massive data storage and collection. Huge amounts of data are caught in the eye of cyberattack, whereas nefarious use or unauthorized information exchange among internal users can also severely undermine consumer privacy.[31] The consolidation of personal information in different touchpoints increases the damage that could be caused in case of any breach and especially when the sensitive behavioural or financial data is concerned.

The other risk is the development of the filter-bubble effect, in which algorithmic-based recommendations restrict consumers to different products or opinions by strengthening the existing preferences. When presented repeatedly and in accordance with previous behaviour, AI systems can reduce the range of choices offered to consumers and limit the diversity of information.[32] This can also create a distortion in the competitive market where some sellers or products will be more favoured than others thus this removes the freedom of the consumer to make an informed and autonomous decision. Another threat of AI personalization is discriminatory outcomes. Algorithms that are conditioned on skewed or non-representative data can reproduce and increase social inequalities.[33] This can be in the form of exclusionary recommendations, differentiated pricing, or targeted advertising that will be disadvantageous to certain groups in e-commerce. These results are inconsistent with notions of fairness and non-arbitrariness in the Indian constitutional jurisprudence and consumer protection legislation. The last challenge to accountability is the unaccountability of AI-based

[30] Pratiksha Baxi, 'Algorithmic Discrimination in Digital Markets' (2022) 4 *NUJS Law Review* 233.
[31] B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) 41.
[32] Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (Penguin 2011) 9.
[33] Anupam Chander, 'The Racist Algorithm?' (2017) 115 *Michigan Law Review* 1023.

personalization that is not explainable and transparent. Customers seldom receive any recognizable clarifications regarding the reason why specific recommendations are given or the pricing strategy applied. This lack of explanation dispels informed consent and erodes the capacity of consumers to challenge or oppose algorithmic decisions that have a negative impact on them.[34] Regulatory perspective is that, with the lack of transparency, the effective control and enforcement practices become difficult, as the authorities may find it hard to evaluate the adherence to the law.

Overall, the AI customization in e-commerce is based on the complex technical processes of the data pipe, the recommendation algorithm, and the dynamic pricing model. Although such systems present serious commercial and experience advantages, they also create huge risks associated with privacy, discrimination, market fairness, and transparency. To deal with these risks, it is not just necessary to implement technological protection but also to install strong legal frameworks that would ensure accountability and protection of consumers by algorithms. As AI-driven personalization continues to shape digital marketplaces, aligning technical innovation with legal and ethical standards will be crucial to sustaining trust and legitimacy in India's e-commerce ecosystem.

Operationalising Legal Compliance in AI-Driven E-Commerce Platforms

The implementation of the artificial intelligence-driven personalization systems in online retail requires a systematic regulation framework that converts the statutory requirements into the working practice. The Digital Personal Data Protection Act, 2023 (DPDPA) in India offers the main legal framework in the regulation of the collection, processing, and retention of personal data utilized in AI-based recommendation and pricing systems. This makes compliance mapping a vital undertaking to an e-commerce organization, so that technological innovation does not drift out of its course in terms of adhering to data protection ideals, consumer rights, and constitutional values. According to the DPDPA, the processing of personal data should have a legitimate basis, i.e. consent or other legitimate purpose.[35] The consent under the Act should be free, specific, informed, and unambiguous, and thus, the e-commerce platform must clearly inform consumers of the intended uses of their data to be used to enhance the AI-based personalization. In the case of consent relying, it should be very

[34] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR' (2017) 7 *International Data Privacy Law* 76.
[35] Digital Personal Data Protection Act, 2023, ss 6–7.

specific to the practices of behavioural profiling, personalized recommendations, and dynamic pricing. Conversely, legitimate use, which is commonly synonymous with legitimate interest, allows limited processing without express authorization, under statutory protection, and in light of common sense sensibilities of the data principal.[36] In the case of AI systems, which significantly impact consumer choice or prices, the fair use without disclosure can be the source of non-compliance with the fairness provision of the DPDPA.

Another fundamental compliance requirement is the limitation of purpose. DPDPA requires that any personal data must be processed on the basis of legality, express, and defined purposes only.[37] Within the AI personalization paradigm, this means that transactional generated data cannot be unreasonably reused to make algorithms profile themselves or specifically target advertising without proper disclosure and consent. The purposive creep, which is the gradual use of data towards other secondary or unrelated purposes, compromises compliance with the statute and consumer confidence. E-commerce organizations, therefore, should record and substantiate every AI application in well-differentiated purposes. It is also closely connected to the limitation of purpose which is the principle of data minimization and storage limitation. Although AI systems are capable of storing all the data, they must only keep that information that is critically required to make recommendations or enhance services provision.[38] The historical retention of behavioural information especially where it is no longer used as an active recommendation factor heightens the chances of privacy invasion and legal infractions. Reducing retention is not only more important to improve data security but also corresponds to the proportionality clause inherent in the Indian privacy jurisprudence.

Regular audits of algorithms can be seen as a form of bias mitigation, which is a new but necessary aspect of compliance mapping. Because of skewed data sets or incorrect model architecture, AI-driven personalization systems can be completely biased or discriminative. Periodic auditing based on such fairness indicators as demographic parity or equal opportunity allows platforms to detect and address discriminatory trends.[39] The DPDPA does not specify that the audits are required to be algorithmic; however, this is aligned with the requirement of the fair and reasonable processing present in the Act. Bias audits also strengthen the adherence

---

[36] Apar Gupta, 'Legitimate Use and Consent under India's DPDP Act' (2023) 65 *Journal of the Indian Law Institute* 178.
[37] Digital Personal Data Protection Act, 2023, s 5.
[38] B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018) 43.
[39] Barocas, Hardt & Narayanan, *Fairness and Machine Learning* (2019) 112.

to the constitutional equality principles and consumer protection principles. Another principle of lawful AI implementation in e-commerce is transparency. In the DPDPA, data fiduciaries must present clear and meaningful information on data processing operations.[40] This, according to AI recommendations, is to provide intelligible explanations to consumers regarding the logic, rationale, and possible implications of automated decision-making. Complete disclosure of the algorithm is unlikely to be a feasible option; however, significant transparency can help maximize informed consent and allows the consumer to exercise his or her rights.

A short analysis of Flipkart style compliance snapshot will demonstrate the real issues of operationalising them. Browsing history, purchase history and device identifiers are the information which e-commerce platforms usually gather, and implement hybrid models with collaborative filtering and deep neural networks. Nevertheless, non-compliance can occur in places where individualized price change is introduced without prior agreed approval or the absence of an audit trail to determine algorithmic bias. These loopholes open platforms to regulatory risk as per the DPDPA and the consumer protection law. Finally, to implement efficient compliance mapping e-commerce companies should incorporate the elements of law into the technical architecture and regulation of AI systems. Legal basis recognition, intent restriction, data reduction, prejudice reviewing, and disclosure should act as mutually reinforcing parts of responsible AI management.[41] Implementing these protective measures into AI-based personalization systems would allow overcoming a legal risk and increasing consumer confidence and responsibility in the dynamic e-commerce market of India.

Towards a Rights-Centric Governance Framework for AI-Driven E-Commerce

The growing use of artificial intelligence in personalization and decision-making in e-commerce requires a systematic form of governance that has legal adherence, ethical considerations, and institutional responsibility integrated into the process of designing and implementing artificial intelligence systems. A rights-based governance system is crucial in order to make sure that technological innovation cannot take away the privacy, equality, or autonomy of consumers, at the same time allowing market efficiencies and competition. This type of framework has to work at the crossroads of the data protection law, consumer protection principles, and competition regulation. One of the underlying components of this form of governance is the embrace of privacy-by-design in AI systems. Privacy-by-design means that

[40] Digital Personal Data Protection Act, 2023, s 8.
[41] Shubha Ghosh, 'Algorithmic Accountability in Indian E-Commerce' (2022) 7 *Indian Journal of Law and Technology* 91.

data protection principles must be incorporated into the design of AI technologies at the early phases of development and be treated as components of compliance equally to other aspects of the design.[42] Under e-commerce this would involve including explicit consent flows, anonymisation or pseudonymisation mechanisms and a stringent purpose limitation mechanisms during design. Implementing such measures puts AI systems in line with the specifications of the Digital Personal Data Protection Act, 2023 and proportionality principles expressed in Article 21 of the Constitution. Privacy-by-design aims at limiting the potential threat of rights abuses and maximising consumer trust in online products and services by reducing the unwarranted exposure of personal data and limiting the secondary use of personal information.

The second component of the suggested model of governance is the creation of the effective system of auditing bias. The use of AI-based personalization systems is prone to delivering discriminatory results because of biased data or incorrect model presuppositions. Such risks may be identified with the help of regular fairness audits that should be performed every quarter and reduce their impact by comparing the outputs of the algorithms with established fairness metrics.[43] Accountability is further enhanced by the use of third-party auditors and certification systems which bring in objectivity and credibility in audit procedures. Despite the fact that the Indian law does not yet oblige the conduct of the audits of the algorithms, the conduct is aligned with the principles of the constitutional equality and the latest tendencies of the world on the responsible AI governance. A third basic element of the governance is an effective dispute resolution mechanisms. Considering the non-transparency of AI-based decisions, consumers need to have effective and easy channels of appealing against automated results that have a negative impact on them. The in-app grievance redressal measures, as well as the presence of clear information about the rights and remedies of users, promote procedural fairness and conform to the Indian law requirements of consumer protection.[44] The transparency of dispute resolution processes also plays a role in algorithmic accountability as it helps platforms to recognize systemic problems and better AI system design in response to consumer feedback.

Lastly, a regulatory sandbox mechanism is a reasonable solution to the issue of balancing between innovation and control. Regulatory sandboxes enable e-commerce platforms to experiment with new AI-based services in a limited condition under the inspection of

[42] Ann Cavoukian, 'Privacy by Design: The 7 Foundational Principles' (2011) *Information and Privacy Commissioner of Ontario*.
[43] Barocas, Hardt & Narayanan, *Fairness and Machine Learning* (2019) 118.
[44] Consumer Protection Act, 2019, ss 17, 35; Consumer Protection (E-Commerce) Rules, 2020.

concerned authorities including the Data Protection Authority and the Competition Commission of India.[45] This will allow experimentation and at the same time allow regulators to evaluate the risk that could be associated with the data protection, market fairness and consumer welfare. The sandboxes enhance adaptive regulation and evidence-based policymaking in the rapidly changing AI environment through dialogue between regulators and industry participants.

To sum up, a rights-based approach to the governance of AI-based e-commerce should include privacy-by-design, bias auditing, effective adjudication, and regulatory experimentation. Cumulatively, these factors make up an institutional structure that protects constitutional and consumer rights without restricting the technological innovation. With the growth of AI personalization as an inseparably part of the digital marketplace, the implementation of these types of governance will play a critical role in making e-commerce in India sustainable, more fair, and accountable.

Conclusion

Personalisation using AI has a great potential to be efficient, convenient to the consumer, and innovative in the market environment of the digital economy; its application must, nevertheless, be well grounded in the constitutional values of India. With the increasing mediation of consumer choice, pricing, and access to digital markets by algorithmic systems, the principles of privacy, equality, and autonomy are being increasingly demanded. The changing regulatory environment in India especially harmonization of data protection standards, consumer protection and constitutional jurisprudence give the normative basis to the creation of responsible and accountable AI systems. When applied in harmony with Fundamental Rights, such regulatory tools can help reduce the risks of surveillance, obscurity and discrimination that AI-driven personalisation introduces. The proposed three-pillar model of governance provides a feasible compromise on the encouragement of technological innovation and protection of individual rights with the establishment of privacy-by-design, fairness, and institutional control in the AI governance. With this kind of solution, it is not only that the development of AI-enabled e-commerce can be economically efficient, but that it is also constitutionally legitimate and socially sustainable.

[45] Competition Commission of India, Market Study on E-Commerce in India (2020) 87.