Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

# Algorithmic Decision Making in Indian E-Commerce: A Legal Analysis under the IT Act, DPDP Act and Consumer Protection Laws

Aboorva S[a] Santhameena S[b]

[a]SASTRA deemed University, Thanjavur, India [b]SASTRA deemed University, Thanjavur, India

*Received* 17 November 2025; *Accepted* 16 December 2025; *Published* 20 December 2025

*This paper investigates the legal complexities surrounding algorithmic decision-making (ADM) in India's digital economy, with a focus on e-commerce. It explores how artificial intelligence and ADM have transformed consumer experiences and business operations through dynamic pricing, targeted recommendations, and operational efficiencies. Despite these benefits, the use of ADM systems raises issues related to data privacy, algorithmic bias, transparency, intermediary liability, and consumer protection. Existing legal frameworks, including the Information Technology Act, the Digital Personal Data Protection Act, and the Consumer Protection Act, are assessed for their effectiveness in addressing these challenges. The paper argues for urgent legal reforms that prioritise accountability, transparency, and fairness in algorithmic decision-making, drawing insights from international regulations and notable Indian judicial precedents.*

**Keywords:** *algorithmic decision-making, artificial intelligence, e-commerce, cyber law, data protection.*

## INTRODUCTION

A new era of dynamic pricing, individualised user experiences, and operational optimisation has been made possible by the development of artificial intelligence (AI) and automated decision-making (ADM), which have profoundly changed India's digital environment, especially in the e-commerce industry. These technological developments have created complicated legal issues pertaining to data privacy, algorithmic bias, transparency, and intermediary responsibility, even while they also have significant positive effects on consumers and businesses. Growing instances of opaque recommendation systems, discriminatory algorithms, hidden pricing, and data breaches highlight the need for laws specifically designed to address the hazards associated with ADM.

Although some fundamental cyber law and data protection issues are addressed by the Information Technology Act, the Digital Personal Data Protection Act, and the Consumer Protection Act, current Indian legal frameworks are still insufficient to meet the complex needs of AI-driven ecosystems. This paper examines the visible and invisible harms caused by ADM in India, assesses the efficacy of current laws, and emphasises the urgent need for specific legal reforms that support accountability, transparency, and fairness in the era of algorithms—all while taking into account international best practices and significant Indian judicial precedents.

## BIG DATA COLLECTION IN E-COMMERCE

In order to better serve the audience, data collection usually entails monitoring customer behaviour across multiple sources. For instance, business owners can see both broad market trends on social media platforms (such as consumers' preference for videos over other types of content) and direct interactions on e-commerce websites (such as clicks on a call-to-action (CTA) button). External data sources, like Hootsuite, or third-party data gathered by organisations that don't deal directly with your audience, are used by e-commerce companies. In order to obtain a thorough understanding of user behaviour, they also gather first-party data using instruments such as customer relationship management (CRM) software. CRM replaces the spreadsheets, documents, and apps that companies frequently use to track customer data by gathering and storing customer information, activity, and communications in a centralised and easily accessible database.[1]

[1] 'Big-Data Ecommerce Explained: How to Use Big Data' (*Shopify*, 03 December 2024) <https://www.shopify.com/blog/big-data-ecommerce> accessed 07 November 2025

Big data sources in e-commerce —

**Transactional Data:** This is an invaluable resource that records the buyer's ID, product ID, transaction time, customer personal information, and cost.

**Social Data:** Some social media users purchase straight through social media platforms, and the majority of online shoppers say that social media influences their decision to buy. This is a clever finding that collects information from social networking sites, such as posts, likes, shares, hashtags, and geographical information, that can affect judgments about what to buy.

**Third-Party Integration Data:** As part of their business strategy, several software entrepreneurs give e-commerce retailers access to large data platforms. E-Commerce startups can bridge the gap in their own historical data and draw in more new prospects by integrating with third-party data vendors in response to trends.

**Behavioural Data:** It records how users engage with a website, including their search queries, things seen, browsing history, and the amount of time spent on sites.[2]

According to the Information Technology Act, people's data is now online and susceptible to misuse due to the expansion of the internet. Big data study indicates that people's searches can be utilised to influence their decisions by examining their search patterns.

## AUTOMATED DECISION MAKING (ADM) SYSTEM

Artificial intelligence (AI) and the abundance of data available have given brands the ability to satisfy consumer preferences on a never-before-seen scale. E-commerce platforms' customer interactions are being revolutionised by AI and Big Data, which makes personalisation more advanced, efficient, and quick. In the past, e-commerce personalisation was restricted to simple tactics like using customers' names in emails or making product recommendations based on past purchases. However, the requirement for more personalised and real-time interactions has grown along with client expectations. Customers now anticipate that businesses will comprehend their needs, make pertinent recommendations, and provide seamless experiences across a variety of touchpoints.[3]

[2] Darya Efimova, 'Big Data in eCommerce: Does It Cost a King's Ransom?' (*EPAM*, 18 June 2024) <https://startups.epam.com/blog/big-data-ecommerce> accessed 07 November 2025

[3] S. Aditya, 'An Overview of E-Commerce Under Cyber Law' (*iPleaders*, 03 June 2020) <https://blog.ipleaders.in/an-overview-on-e-commerce/> accessed 07 November 2025

Big Data and AI can help with this. AI is now more capable than ever of comprehending and forecasting consumer behaviours, preferences, and aspirations by evaluating enormous datasets. The automation of numerous workflows in inventory management, order fulfilment, customer support, dynamic price adjustments, and many other procedures was made possible by big data and the capacity to process it in real-time[4]. Almost 80% of marketing automation users benefit from growth in leads and conversions, and it's found that customer retention rate may grow up to 90% with automated retention marketing campaigns.

Startup founders can free up time for strategic tasks, pitching, and investor communication by using big data to automate operations. By demonstrating that all of their choices are informed by data, they also improve their prospects of obtaining additional funding.

## PERSONALIZATION IN E-COMMERCE

**Product Recommendations:** This is one of the most obvious ways that AI and Big Data impact e-commerce personalisation. Artificial intelligence (AI) algorithms can forecast which products are most likely to appeal to each buyer by examining their browsing habits, past purchases, and even in-the-moment interactions.

**Marketing:** Content and marketing techniques can benefit from personalisation. E-commerce platforms may now develop tailored deals, targeted advertisements, and personalised email campaigns that appeal to specific consumers. These can be sent according to demographics, location, time of day, and even historical conduct.

**Chatbox and Customer Service:** Chatbots and virtual assistants driven by AI have completely changed e-commerce customer service. These AI-driven systems can give individualised support by identifying patterns in client requests, anticipating problems, and providing solutions that are specific to each customer's needs through the use of machine learning algorithms and natural language processing (NLP).

**Dynamic Pricing Strategy:** AI and big data enable e-commerce platforms to modify prices in response to consumer behaviour, competition, and demand. AI systems can provide

[4] 'Personalization With AI and Big Data in E-Commerce' (*Prescience*, 12 September 2024) <https://presciencedS.com/personalization-with-ai-and-big-data-in-e-commerce/> accessed 07 November 2025

individualised pricing to each consumer by analysing their purchase habits and external variables like the time of day, the weather, and their location.

**Navigation and Search Results:** AI-powered search engines are able to learn from user interactions and gradually improve the search experience to show the most pertinent results. Customers can find what they're seeking faster and with greater accuracy by using predictive search capabilities that provide product recommendations based on past inquiries. By examining consumer behaviour and displaying customised homepages, product categories, or even checkout processes, AI can also improve website navigation. This results in a more seamless, user-friendly purchasing experience that suits personal tastes.[5]

## CHALLENGES FACED BY CONSUMERS

**Hidden Costs:** According to a recent Baymard Institute survey, 49% of UK online buyers leave their carts empty because the additional expenses, such as shipping, taxes, and fees, are too expensive. A pleasant shopping trip can quickly become a frustrating one when these expenses are discovered at the last minute. The customer perceives it as a betrayal of confidence. After spending time selecting the goods and determining that your website is the ideal place to buy them, they discover at the last minute that an unforeseen fee has suddenly appeared.[6]

**Lack of Pricing Transparency:** The price does not clearly indicate which costs are for shipping, VAT, GST, and other factors that affect the total cost.

**Discrimination:** E-commerce websites employ algorithms to alter rates for various customers according to their information (such as location, browsing history, recent purchases, online buying level, and willingness to pay), which may result in customers being overcharged without their knowledge. Customers may start to think that this is discriminatory.

**Subscription Traps:** This trend entails customers being automatically enrolled in subscription services without explicit notice following free trials. Many businesses

[5] *Ibid*
[6] 'Why You Are Losing Sales: The Impact of Hidden Costs on E-commerce Platforms' (*Blue Wave Concepts*, 13 December 2024) <https://www.bluewaveconcepts.com/why-you-are-losing-sales-the-impact-of-hidden-costs-on-e-commerce-platforms/> accessed 07 November 2025

purposefully complicate the cancellation process so that consumers must follow several steps or contact customer support by phone.

**Loss of Trust and Brand Reputation:** Consumers lost trust in the retailer as a result of deceptive pricing, hidden costs, and a lack of transparency, which affected the company's credibility and caused long-term problems.

## LEGAL ASPECTS IN INDIA

**Information Technology Act, 2000:** The importance of the internet in our lives has increased incredibly quickly in recent years. Since most business transactions (buying, selling) take place regularly, our web presence has grown along with our activities. E-commerce is here to stay, as demonstrated above. But it's also a sector that is particularly susceptible to cybercrime, which is growing just as quickly as e-commerce. In other words, cybercrime is the use of computer resources for illegal or unauthorised purposes. Every day, enormous volumes of money and information are transferred via e-commerce platforms, necessitating strict security because customer data is vital to an organisation's success.

Criminals use malware or malicious software to target computer systems, taking control of the machine and gaining access to sensitive data stored on it without the users' knowledge, or they trade valuable stolen financial information from millions of unwitting internet users on the online black market.

The main piece of legislation in India that controls cybercrime and electronic trade is the Information Technology Act, 2000 (IT Act).[7] This law's main goal was to implement the 1996 publication of the UNCITRAL Model Law[8] on Electronic Commerce (E Commerce Law). Giving legal legitimacy to online transactions and enabling the transfer of electronic data over electronic communication channels (e-commerce) were the main goals of this Act. In addition to defining punishments for cybercrime and other offences, the Act creates a regulatory structure. In the interest of Indian sovereignty and integrity, Indian defence, and state security, it permits the Centre to prevent the general public from accessing an intermediary[9].

[7] Information Technology Act 2000

[8] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996

[9] Priyanka Barik, 'Cyber Law's Emerging Role In Indian E-Commerce' (*King Stubb & Kasiva*, 04 January 2022) <https://ksandk.com/regulatory/indian-e-commerce-law-under-cyber-law/> accessed 07 November 2025

This demonstrates how widespread the internet is today as a marketplace where a huge number of individuals purchase and sell goods every day. Online buying can occur through direct purchases or transactions made through agents or affiliates. Online selling can be done through social networking sites, auction websites, or your own website. Regarding business technology, the growth of e-commerce has created a marketplace for the purchase and sale of goods and services in addition to powering vital internal corporate processes. E-commerce inherently raises challenges with copyright, data security, and compliance. First off, intellectual property rights are among the most crucial concerns for any company doing business online, including e-commerce, or entering into an e-contract. IPR (Intellectual Property Rights) protection is a big problem and a barrier in e-business because the Internet is so vast, difficult to govern, and has so few laws addressing safety and protection. Second, it is almost impossible to carry out an online purchase without obtaining some kind of user personal data, which may also constitute a privacy violation.

**Section 43 of the IT Act:** Several actions that are illegal under law if performed without the owner of the computer system's agreement are listed in Chapter IX, Section 43, of the IT Act of 2000.[10] These acts are discussed below –

- Programming code theft or interference
- Introducing viruses or other malicious software into the system
- Charging someone for services they haven't used
- Altering or damaging information to reduce its value, or causing harm
- Downloading or copying data with the proper authorisation
- Helping others break the law[11]

An insider or hacker manipulates an algorithmic mechanism in an e-commerce platform. They modify the recommendation engine for malevolent purposes, obtain unauthorised access, or change the code or data to make some goods more expensive for specific customer segments. A vendor or supplier may occasionally alter their pricing model or manipulate the system for personal benefit by breaking into the platform's algorithm to view the prices of

[10] Information Technology Act 2000, s 43

[11] 'Understanding the Information Technology Act, 2000 in E-commerce' (*Lloyd Law College*) <https://www.lloydlawcollege.edu.in/blog/it-act-2000-ecommerce-legal-framework.html> accessed 07 November 2025

their competitors. This is covered by Section 43 of the IT Act,[12] and unauthorised access carries legal liability.

**Section 66 of the IT Act:** Computer-related offences are included under Section 66. Any individual who commits any of the acts listed in Section 43 dishonestly or fraudulently faces a maximum sentence of three years in prison, a maximum fine of five lakh rupees, or both. When someone violates Section 43 with the intention of causing wrongful loss, wrongful gain, or dishonesty, Section 66 is applicable. The criminal faces a maximum sentence of three years in prison, a fine, or both. If someone engages in any of the behaviours specified in Section 43 with the intent to conduct fraud or dishonesty, they shall be held accountable. Penalty: a fine of up to Rs. 5 lakh, three years in prison, or both.

If a pricing algorithm is tampered with the intention of making erroneous profits. If a vendor, for instance, alters recommendation decisions to deceive customers or manipulates the algorithm to provide itself a pricing advantage, then Section 66 may be applicable. Intention is the distinction between Sections 43 and 66.[13] Civil liability is covered by Section 43, including for careless or inadvertent unlawful acts. Even if someone gains access to or interferes with a system without authorisation, they still have to pay the victim. However, Section 66 necessitates dishonest or fraudulent intent. When committed for illegal purposes, the same behaviours are punishable by jail time and penalties. Therefore, although Section 66 is punitive, Section 43 is preventive and compensatory. Collectively, they address the criminal and civil facets of cybercrimes.[14]

**Mphasis BPO (Citibank Call Centre) Fraud, 2005:[15]** Four Mphasis BPO workers unlawfully obtained private client information from Citibank's internal systems, including account information and PIN codes. The workers transferred around $426,000 (approximately ₹3 crores) from Citibank accounts located in the United States to fictitious Indian bank accounts made with fraudulent documentation by manipulating data systems and utilising digital

[12] Information Technology Act 2000, s 43

[13] Information Technology Act 2000, ss 43, 66

[14] 'Punishments Under Section 43 of the IT Act with Real-Life Examples' (*Apni Law*) <https://www.apnilaw.com/legal-articles/acts/punishments-under-section-43-of-the-it-act-with-real-life-examples/?utm_source=chatgpt.com> accessed 07 November 2025

[15] Abhay Vaidya, 'India's First BPO Scam unraveled' *The Times of India* (23 April 2005) <https://timesofindia.indiatimes.com/home/sunday-times/deep-focus/Indias-first-BPO-scam-unraveled/articleshow/1086438.cms> accessed 07 November 2025

access passwords. When Citibank's automated transaction monitoring system—an early ADM tool—identified odd money transfers across unrelated accounts, the fraud was discovered. According to Sections 43 and 66, they are held half accountable. The employees were charged with computer fraud, data theft, and criminal breach of trust, and the police were able to recover almost $230,000.

ADM played two roles in this instance: a positive role and a negative role. The upside is that it demonstrated ADM's function in risk identification by assisting in the detection of the anomalous transactions using algorithmic fraud detection methods. Employees could override or get around algorithmic safeguards because Citibank's automated systems lacked robust algorithmic access control.[16]

**Reliance Jio Data Theft Case:[17]** An important turning point in the history of digital governance in India was the Reliance Jio Data Theft Case (2017). The website Magicapk.com allegedly exposed the names, cellphone numbers, and Aadhaar information of more than 100 million customers. The business reported the illegal access and data extraction under Section 43 and the dishonest and fraudulent abuse of data under Section 66. The event demonstrated the critical need for more robust cyber law enforcement and revealed significant weaknesses in telecom data protection.

This vulnerability had more profound ramifications from the standpoint of Algorithmic Decision-Making (ADM). In order to operate recommendation engines, customised pricing schemes, and customer analytics, e-commerce and telecom platforms require precise and secure consumer data. Algorithms that use compromised data may generate unfair, prejudiced, or exploitative results, resulting in unseen harms, including mis-profiling and unfavourable consumer treatment. The case argues for extending India's cyber law framework beyond intermediary liability to include algorithmic responsibility and shows how data vulnerability directly compromises algorithmic fairness. In order to guarantee that ADM in e-commerce functions morally and protects consumer rights, it highlights the importance of data protection, transparency audits, and accountability procedures.

[16] Punishments Under Section 43 of the IT Act with Real-Life Examples (n 14)

[17] Srinath Rao, 'Reliance Jio data breach: Police register complaint' *The Indian Express* (12 July 2017) <https://indianexpress.com/article/business/reliance-jio-data-breach-police-register-complaint-4746445/> accessed 07 November 2025

**Kumar v Whiteley (BSNL Broadband Case):**[18] This case shows how algorithmic systems, including e-commerce data management and automated billing, can be compromised by illegal access or data manipulation. This instance serves as an example of the "visible harms" brought about by "invisible algorithmic manipulations," in which tainted data skews automated results and causes monetary loss. It highlights that although the Information Technology Act of 2000, India's present cyber law framework, is effective in punishing unauthorised access, it does not have specific laws controlling algorithmic accountability or data-driven decision-making. Thus, this case bolsters the research thesis that algorithmic transparency, auditability, and fairness norms inside e-commerce systems should be included in legal reforms that go beyond access-based liability (Sections 43 and 66).

**S. Sekar v The Principal General Manager (Telecom) (BSNL):**[19] The petitioner in this case (Madras High Court, 2007) contested an exaggerated broadband bill produced by BSNL's automated system, claiming either a system fault or unauthorised access. BSNL defended its stance by claiming that its servers' algorithmic logs served as the basis for the charge. The Court ruled that although automation increases productivity, service providers must guarantee that algorithmic processes are accurate and transparent since customers cannot be punished for inexplicable algorithmic or technological errors. In the context of India's developing cyber and e-commerce legal environment, this case emphasises the early ramifications of algorithmic decision-making (ADM) in digital services, highlighting the necessity of accountability and human control in automated systems.

**Section 66A of the IT Act:** The Information Technology Act of 2000 made it illegal to send "offensive," "menacing," or "false" messages via electronic communication (Section 66A). Despite being designed to stop online abuse and false information, it gained notoriety for having ambiguous language that allowed for abuse and overreach. The Supreme Court ruled in ***Shreya Singhal v Union of India***[20] ***(2015)*** that Section 66A was unconstitutional because it restricted free speech without providing sufficient protections, in violation of Article 19(1)(a) of the Constitution.[21]

[18] Hema Modi, 'All you need to know about hacking' (*iPleaders*, 23 October 2021) <https://blog.ipleaders.in/all-you-need-to-know-about-hacking/> accessed 07 November 2025

[19] *S. Sekar v The Principal General Manager (Telecom) (BSNL)* WP (MD) No 10208/2005 & MP No 10905/2005

[20] *Shreya Singhal v Union of India* AIR 2015 SC 1523

[21] Constitution of India 1950, art 19(1)(a)

The deletion of Section 66A brings to light a crucial issue in regulating online behaviour from the perspective of algorithmic decision-making (ADM) in e-commerce: the requirement for legal accuracy when defining liability and harm in digital systems. Because they rely on opaque data models, automated algorithms that identify "offensive" or "false" information frequently reinforce bias or stifle free speech. The case serves as a reminder of how vague legal requirements can result in capricious algorithmic enforcement, leading to "visible harms" including market distortion and content manipulation. In order to balance innovation, free speech, and consumer protection in India's digital economy, ADM frameworks must include clear, responsible, and open regulatory processes, as the Section 66A experience shows.

**Section 66B of the IT Act:** The consequences for unfairly obtaining stolen computer data or communication devices are covered in Section 66B of the Information Technology Act 2000. A maximum term of three years in prison, a fine of up to one lakh rupees, or both could be imposed on anyone discovered in possession of stolen computer resources or communication equipment.

**Section 67A of the IT Act:** Section 67A covers the penalty for publishing and spreading e-material that contains sexually explicit content. When someone is convicted under Section 67A[22], they might be fined up to Rs. 5 lakh and imprisoned for up to 3 years on their first conviction. If they are caught a second or subsequent time, they could be fined up to Rs. 10 lakh and imprisoned for up to 5 years.

Information disclosure in violation of a valid contract is punishable under Section 72A[23] of the Amendment Act 2008.[24]

## INTERMEDIARY LIABILITY

A person who receives, stores, transmits, or provides any services related to a specific electronic record on behalf of another person is considered an intermediary, according to Section 2(w)[25]. This includes telecom service providers, network service providers, internet

[22] Information Technology Act 2000, s 67A
[23] Information Technology Act 2000, s 72A
[24] Information Technology (Amendment) Act 2008
[25] Information Technology Act 2000, s 2(w)

service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online marketplaces, and cyber cafes.[26]

The Information Technology Act of 2000 establishes the idea of 'safe harbour"' to safeguard middlemen in the Indian legal system. This protection was first added in 2000 when the IT Act was amended to amend Section 79, which, as stated in Rule 3[27] of the (Intermediaries Guidelines) Rules, 2011 ('IT Rules'), excludes intermediaries from liability for content created by third parties on their platforms. In the past, intermediaries had to actively seek protection by demonstrating their due diligence and proving their innocence in situations where offences were committed without their knowledge.

The IT Act's Section 79(1)[28] grants intermediaries' immunity for third-party content that they host. Section 79(2) and (3) of the IT Act[29], however, restrict this exemption, stating that it only applies in cases where the intermediary's function is technical and passive. Furthermore, intermediaries who have engaged in any illegal action cannot claim immunity. A 'notice and take down' policy is established by Section 79(3)(b)[30], which mandates that intermediaries delete illegal content as soon as they are made aware of its existence.

Furthermore, IT Rule 3 exempts intermediaries from liability for third-party material by requiring them to exercise due diligence. The publishing of guidelines and policies, such as user agreements and privacy policies, cautioning users against uploading false or misleading information or content that infringes on intellectual property rights, is part of this due diligence. The 'safe harbour' clause in Section 79 is essential for regulating online marketplaces like Amazon, Flipkart, and others in the context of e-commerce. These platforms serve as middlemen, hosting or transmitting third-party data, including ads, product listings, and customer reviews, without actively altering or managing it.

As long as they act as impartial intermediaries, e-commerce platforms are exempt from accountability for any illegal or infringing content uploaded by users or sellers under Section

[26] Siddhant Samaiya, 'An Analysis of Intermediary Liability in India and the European Union' (*Manupatra*, 02 September 2024) <https://articles.manupatra.com/article-details/AN-ANALYSIS-OF-INTERMEDIARY-LIABILITY-IN-INDIA-AND-THE-EUROPEAN-UNION> accessed 07 November 2025

[27] Information Technology (Intermediaries Guidelines) Rules 2011, r 3

[28] Information Technology Act 2000, s 79(1)

[29] Information Technology Act 2000, ss 79(2)–(3)

[30] Information Technology Act 2000, s 79(3)(b)

79(1). This protection is conditional, though. According to Sections 79(2) and 79(3), the intermediary loses immunity if they take part in, start, or alter the sale or content, or if they neglect to take down unlawful or infringing materials after being notified. Moreover, e-commerce intermediaries are subject to due diligence requirements under the Information Technology (Intermediaries Guidelines) Rules 2011, specifically Rule 3. Clear privacy rules, conditions of use, and cautions against the sale of fake goods, misleading advertising, and intellectual property rights infringement must all be prominently displayed. If these responsibilities are not met, the platform may lose its safe harbour status and become legally liable.

The IT Act's safe harbour system essentially strikes a balance between consumer protection and the operational flexibility of e-commerce intermediaries by guaranteeing accountability without impeding innovation. It guarantees that although platforms are protected from user-generated wrongdoing, they are still in charge of upholding transparency and acting quickly to address infractions when they are discovered.

**Shreya Singhal v Union of India:**[31] The ruling in Shreya Singhal v Union of India (2015) by the Supreme Court profoundly altered intermediary liability in India and had an immediate impact on the operation of automated decision-making (ADM) in e-commerce. Citing its ambiguous and capricious limitations on online speech, Section 66A of the Information Technology Act, 2000, was mainly invalidated for violating Article 19(1)(a).[32]

More significantly, the Court provided clarification on the application of Section 79[33], the safe harbour provision that shields middlemen like e-commerce sites from responsibility for content created by third parties. It ruled that intermediaries are not required to remove content on the basis of individual complaints, but only in response to a valid order from a court or government agency. This guarantees that automated mechanisms won't compel platforms to impose undue censorship.

This decision offers legal consistency for e-commerce firms that use ADM, such as algorithms that screen reviews, censor content, or suggest items. It affirms that intermediaries are protected from liability unless they willfully disobey court orders or government mandates,

[31] *Shreya Singhal v Union of India* AIR 2015 SC 1523
[32] Constitution of India 1950, art 19(1)(a)
[33] Information Technology Act 2000, s 79

striking a balance between innovation and accountability. The ruling highlights the fact that automation does not release intermediaries from their legal obligations. To avoid abuse or damage, platforms using ADM must maintain human oversight and guarantee adherence to due diligence requirements. Therefore, the case demands accountability and transparency in automated e-commerce operations, reaffirming that intermediary liability still applies even in algorithm-driven systems.

## DIGITAL PERSONAL DATA PROTECTION (DPDP) 2023

With consent at the core of its compliance system, the Digital Personal Data Protection (DPDP) Act 2023 establishes a comprehensive regime for the protection and legal processing of digital personal data in India. For industries like e-commerce, where automated decision-making (ADM) and extensive data processing are prevalent, this rule is especially important. The main clauses about processing, consent, accountability, and supervision for algorithmic use in e-commerce and other industries are listed below.

**Consent and Notice Requirements:** Unless there are specific authorised state or legal purposes, data fiduciaries (such as e-commerce platforms) must get individuals' (also known as 'data principals') valid, explicit, and informed consent before processing any personal data. Silence or pre-checked boxes are not acceptable forms of consent; instead, it must be free, explicit, informed, unconditional, and given by a clear affirmative action. Data principals must get clear, unambiguous notice in plain English of the types of personal data that are gathered, their intended uses, grievance procedures, and ways that they can exercise their rights. Notifications must be simple to comprehend and presented separately from other data.[34]

**Lawful Purpose and Limitation:** Personal information may only be processed for legitimate purposes that were made clear to the individual at the time of acquisition; subsequent uses cannot go beyond these initial, established goals.[35]

[34] Information Technology Act 2000, s 6

[35] Information Technology Act 2000, s 4

**Rights of Data Principals:** The legislation gives people the ability to examine what information is kept about them, request that inaccurate or out-of-date data be corrected or erased, and quickly revoke consent.[36]

**Significant Data Fiduciaries (SDFs):** These are organisations that process huge amounts of sensitive data or that profile individuals. Mandatory data protection impact assessments, the hiring of data security officers, recurring audits, and increased transparency for high-risk processing—like recommendation engines or dynamic pricing algorithms—are among the increased responsibilities placed on SDFs.[37]

**Enforcement and Penalties:** For severe non-compliance (such as data breaches or misuse), the Data Protection Board of India has the authority to enforce the Act, look into violations, order corrective measures, and levy fines of up to ₹250 crore. In public interest instances, entities are required to prevent access, comply with information requests, and notify violations as soon as possible.[38]

As algorithmic decision-making in e-commerce frequently depends on extensive data gathering and computerised profiling, the processing and consent/notice provisions (Sections 4, 5, 6) are essential. The Act's standards for informed consent and authorised purpose serve as a safeguard against algorithmic pricing or targeting that lacks transparency. Regulation of algorithmic systems is gaining traction because the idea of a Significant Data Fiduciary and additional responsibilities (Section 10) is in line with the concerns presented by large platforms that use ADM for recommendation engines or dynamic pricing. The consumer has recourse against harms caused by algorithmic processing (such as inaccurate profiling and biased results) thanks to the rights of data principals (access, correction, and erasure).[39]

Despite having a strong data protection framework, the DPDP Act does not yet specifically address advanced AI concerns like algorithmic fairness, real-time surveillance, or transparency rules for automated profiling. Although there are increasing calls for clear

[36] Information Technology Act 2000, s 5
[37] Information Technology Act 2000, s 10
[38] The Digital Personal Data Protection Act 2023
[39] Anahad Narain, 'What Are the Grounds for Processing under the DPDP Act' (*Consentin*, 04 July 2025) <https://www.consent.in/blog/grounds-for-processing> accessed 07 November 2025

algorithmic responsibility and transparency, the duties now placed on data fiduciaries only partially address issues unique to AI.

## CONSUMER PROTECTION (E-COMMERCE) RULES,2020

In India, e-commerce is governed under the Consumer Protection (E-Commerce) Rules, 2020. Through the disclosure of the product's country of origin, price, return policy, and seller information by e-commerce firms, these regulations create a framework that safeguards consumer rights and transparency in e-commerce. Furthermore, it requires the establishment of an officer to oversee complaints resulting from consumer transactions. False or misleading advertisements and the sale of counterfeit goods are examples of unfair trade practices that are forbidden. Under the Consumer Protection Act, noncompliance would result in fines and limitations on corporate operations. This suggests that avoiding violations is more important for maintaining consumer trust and legal standing.[40]

## CONSUMER PROTECTION ACT, 2019

Any democratic society must uphold the fundamental right to privacy. 'The ability of the individual to determine for himself/herself the time, situation, and degree to which his/her attitudes, beliefs, behaviour, and opinion are to be shared with or withheld from others' is the definition of disclosural privacy. The Consumer Protection Act was created to protect the interests of India's expanding e-commerce customers. It creates mechanisms for addressing faulty products or services and encourages openness in internet interactions. E-commerce websites are required by the legislation to provide detailed information about their goods and services, including costs and return guidelines. Additionally, it forbids unfair business practices such as deceptive advertising and fraudulent sales. A clear return policy reduces disagreements and expedites the process of resolving them, which increases customer loyalty.

The comparatively more prevalent forms of dark patterns on e-commerce websites and applications include fabricating a sense of urgency, producing social proof, default option

[40] Ajay Lulla, 'The Legal Aspects of Online Business and E-Commerce' (*King Stubb & Kasiva*, 30 September 2024) <https://ksandk.com/e-commerce/legal-aspects-online-business-and-e-commerce/> accessed 07 November 2025

preselection, masking ads, requiring a purchase registration, or persistently reminding users to buy items in their cart.

Under Section 18 of the Consumer Protection Act 2019, the Department of Consumer Affairs (DoCA) released Guidelines for Prevention and Regulation of Dark Patterns in order to combat these concerns. These regulations seek to prevent the adoption of misleading design patterns that infringe upon consumer rights and protect consumers from unfair commercial practices in e-commerce. As outlined in the Digital Personal Data Protection (DPDP) Act 2023 and its supplemental regulations, this is consistent with the government's larger initiatives to restrict data usage for particular purposes.

## INTELLECTUAL PROPERTY RIGHTS (IPR)

The Internet essentially disregards territorial boundary distinctions. Thus, the Internet has been referred to as 'the biggest copy machine in the world.' Trademarks, copyrights, patents, and designs created by individuals and companies in the e-commerce industry are protected against unlawful use by Intellectual Property Rights (IPR) regulations. E-commerce platforms need to be careful to prevent intellectual property rights violations and the sale of fake goods while facilitating buyer-seller transactions. In terms of legal challenges, monetary fines, and harm to one's reputation, breaking IPR law can have very serious repercussions. Respect for IPR law will safeguard creators' interests and promote innovation.

## PAYMENT AND SETTLEMENT SYSTEMS ACT 2007

The purpose of the Payment and Settlement Systems Act is to regulate the types of payment systems that ensure safe online transactions on e-commerce platforms. The act establishes rules that payment service providers must follow in order to facilitate safe money transfers between buyers and sellers while maintaining a watchful eye out for fraud. E-commerce companies must abide by the rules set forth by the RBI, including all KYC requirements and transaction limits. Tokenisation, which substitutes secure tokens for sensitive card information to safeguard customer data during online transactions, is one of the methods that merchants and payment gateways must use in accordance with RBI rules.[41]

[41] *Ibid*

## INTERNATIONAL ASPECT

**GDPR:** An important legislative framework for data protection and privacy in the digital age is the General Data Protection Regulation (GDPR), which was passed by the European Union in 2018. It is especially important for automated profiling and algorithmic decision-making (ADM), which are becoming more and more important in e-commerce platforms. According to Article 22 of the GDPR, people have the right to be free from decisions that are made purely based on automated processing that have legal or comparable important consequences. This guarantees that human monitoring is still a crucial component of these systems. The "invisible harms" that can occur when algorithms decide on pricing, product display, or customer segmentation are directly countered by this rule, which reflects the values of transparency, fairness, accountability, and data minimisation. Additionally, it requires explainability, which means that users must comprehend the data that goes into automated decision-making.[42]

**CCPA:** Enacted in 2018, the California Consumer Privacy Act (CCPA) is a groundbreaking data privacy law in the US that gives customers substantial control over their personal data. It guarantees the right to access, remove, and refuse the sale or exchange of personal information. Because it limits the unrestricted use of consumer data in automated profiling, targeted advertising, and tailored pricing, practices that frequently result in 'invisible harms' in e-commerce ecosystems, the CCPA is essential when discussing algorithmic decision-making (ADM).[43]

The CCPA's emphasis on data transparency and customer consent indirectly regulates algorithmic processes that depend on extensive data analytics, even while it does not directly regulate ADM. The 2020 California Privacy Rights Act (CPRA) update to the legislation strengthened responsibility for companies using AI-driven decision systems by introducing the right to restrict the use of sensitive personal data.

[42] Sheetal Rangwar, 'Impact of AI on Data and Privacy Protection Laws'(*iPleaders*, 03 July 2024) <https://blog.ipleaders.in/impact-of-ai-on-data-and-privacy-protection-laws/> accessed 07 November 2025

[43] Anas Baig & Aswah Javed, 'What to Know about the New CCPA Regulations on Automated Decision-Making Technology' (*Securiti*, 13 September 2025) <https://securiti.ai/ccpa-automated-decision-making-technology/#:~:text=I.-,Introduction,Protection%20Agency%20(CCPA)%20regulations> accessed 07 November 2025

## CONCLUSION

In terms of regulating cutting-edge technologies, especially artificial intelligence (AI), which is developing at a never-before-seen rate, India is at a turning point. The nation must create a thorough legal framework that covers both the technical and wider societal ramifications of AI in order to guarantee that it serves society responsibly. Algorithmic accountability should be given top priority in this paradigm, requiring companies using AI systems to be open about their decision-making procedures, the data they utilise, and any potential biases these systems may include. By doing this, India may foster trust in digital systems while lowering the possibility of discrimination and unfair treatment that could result from opaque algorithms.

Strong privacy and data protection measures are equally crucial. AI systems are increasingly powered by citizens' personal information, which needs to be protected from exploitation, abuse, and illegal access. In order to ensure that accountability is assigned wherever harm or carelessness happens, the legislative framework must clearly define the legal duties of AI developers, operators, and intermediaries. In order to balance innovation with societal well-being, ethical criteria must be formalised to direct the development, application, and usage of AI technology.

Because they frequently serve as gatekeepers influencing results through algorithms, e-commerce platforms and other digital intermediaries need special attention. Even while these platforms might operate as impartial middlemen, they must be held accountable for their conduct if they deliberately tamper with rankings or outcomes. When norms are broken, regulatory organisations should monitor algorithmic fairness, supervise compliance, and impose corrective actions.

India can protect consumer rights, uphold constitutional values, and promote responsible AI innovation by implementing these extensive measures. In addition to reducing the hazards connected with AI technology, this proactive legal strategy would position India as a pioneer in moral, responsible, and open digital governance, guaranteeing that the advantages of technical growth are fulfilled without sacrificing social values.