CONSUMER PROTECTION IN THE ERA OF ARTIFICIAL INTELLIGENCE: LEGAL CHALLENGES AND REGULATORY RESPONSES

Sonali Debbarma[1] & Dr. Mousumi Kalita[2]

ABSTRACT

The adoption of AI by e-commerce, financial, healthcare and digital services has greatly changed consumer engagement. Even though AI saves time, personalizes and makes things more convenient, it also puts the main concepts of consumer protection at risk. Examples are not knowing how algorithms function, improper use of personal data, biased decision making, tactics used for behavioural control and accountability gaps in AI. These new legal dangers are not always managed perfectly well by the traditional Consumer Protection Act, 2019 and the Information Technology Act, 2000. Although proposals such as the EU's AI Act and OECD's AI Principles exist to guide responsible AI use, gaps continue in making sure these guidelines are properly followed.

It explores how AI influences consumers, identifies weaknesses in existing legal frameworks and determines how well both old and new regulations are dealing with AI. It underlines the immediate requirement for AI-related laws that make sure AI-based systems are clear, fair and responsible. It also suggests the use of algorithmic reviews, assessments of impacts and the creation of separate bodies to supervise the field. Case studies and comparisons in this research try to add to the debate on finding a balance between innovation and consumer interests in the digital arena. In the end, it suggests managing AI by putting th rights of people first and encouraging the ethics of technology.

Keywords: Artificial Intelligence (AI), Consumer Protection, Data Privacy, Algorithmic Bias, Accountability.

[1] Research Scholar, Faculty of Law, ICFAI University, Tripura Kamalghat, Mohanpur, West Tripura-799210
[2] Assistant Professor of Law, Faculty of Law, ICFAI University, Tripura

1. INTRODUCTION

Artificial intelligence (AI) is revolutionizing consumer sectors such as advertising, fintech, e-commerce, and customer service, enabling unprecedented customisation and efficiency while complicating consumer rights in the digital economy. The legal framework must evolve to meet data privacy, manipulation concerns, fairness, and transparency challenges that extend beyond traditional consumer law[3][4][5][6][7][8][9]

Still, strongly integrating AI into businesses generates major worries about safeguarding consumer rights. Because AI tools rely little on human action, there are now major concerns about transparency, unfair bias, using too much data and loss of informed consent. Most consumers do not know how decisions about them are made or if they have been given a fair chance by these systems. Many people doubt that traditional fairness and transparency standards can be followed because AI systems are not designed to work transparently.

Because technology is always changing, the laws currently in place are having trouble dealing with the special problems that AI brings. The Consumer Protection Act, 2019 in India along with the Information Technology Act, 2000 do not meet AI-specific concerns involving algorithms or using technology to make decisions. As a result, better and updated laws should be created that look after people's interests without limiting innovation. This paper focuses on these legal hurdles and recommends solid regulations that will help use AI ethically and responsibly for consumers.

2. RISE OF AI IN CONSUMER MARKETS (ADVERTISING, FINTECH, E-COMMERCE, CUSTOMER SERVICE).

AI can be found everywhere in the advertising industry, facilitating hyper-personalized advertising, predictive analytics, content generation, and real-time optimization of brands.

[3] ASCI ONLINE, https://www.ascionline.in/academy/wp-content/uploads/2025/03/ADNext-Report-digital.pdf (last visited on 6 September, 2025)
[4] PROFESSIONAL AND EXECUTIVE DEVELOPMENT, https://professional.dce.harvard.edu/blog/ai-will-shape-the-future-of-marketing/ (last visited on 6, September, 2025)
[5] DESIGN O WEB, https://designoweb.com/blog-detail/top-use-cases-of-ai-in-fintech-healthcare-and-e-commerce-in-2025 (last visited on 6 September, 2025)
[6] Ms. Sonia Maan and Dr. Ankita Sharma, *Protecting Consumer Rights in the Age of Artificial Intelligence: Legal Implications and Challenges in Consumer Protection*, ADVANCES IN SOCIAL SCIENCE, EDUCATION AND HUMANITIES RESEARCH (last visited on 6, September, 2025)
[7] AISERA, https://aisera.com/blog/ai-in-fintech/ (last visited on 6, September, 2025)
[8] UNCTAD, https://unctad.org/system/files/information-document/ccpb_artificial_intelligence_consumer_protection_en.pdf (last visited on 6 September, 2025)
[9] INDIAAI, https://indiaai.gov.in/article/navigating-the-ai-horizon-safeguarding-consumer-rights-in-the-digital-era (last visited on 6 September, 2025)

Services such as Netflix and Amazon rely on AI to evaluate customer behaviour and suggest content and products that meet their individual preferences. AI is used in fintech to build smarter and safer banking, including detecting frauds, credit scoring, personal financial advice, and real-time compliance and reporting using retch. Some of the applications of AI in e-commerce include dynamic pricing, personalized shopping experience, and automated customer experience with chatbots and recommendation engine. AI-driven chatbots and virtual assistants also revolutionize customer service by providing 24/7 personalized service and minimize human interaction[10].

3.1 ADVERTISING AND MARKETING

Advertising and its algorithms powered by AI has altered the way businesses access consumers. Advanced algorithms can be used to measure consumer behaviour, preferences, and the history of browsing in order to generate hyper-targeted campaigns. Personalization of ad delivery on platforms like Google, YouTube and Meta is performed by recommendation engines, whereas scaling personalized content is created through the use of generative AI. Although this level of accuracy makes the consumer relevant to consumers, there are ethical considerations of autonomy, manipulation and dark patterns in digital marketing[11].

3.2 FINTECH AND CONSUMER FINANCE

AI is used in the financial industry to run credit scores, fraud detection, robot-advisors, and custom banking. The automated decision making is giving quicker and more effective services to consumers, particularly in approvals in credit and investment guidance. Yet, such examples as the Apple Card scandal (2019) demonstrate that algorithmic bias and transparency can be dangerous, and consumers can be deprived of financial opportunities or even discriminated without any clear answers[12].

3.3 E-COMMERCE AND RETAIL

AI is the staple of internet-based e-commerce. AI can help businesses maximize their sales and enhance consumer experiences through dynamic pricing algorithms and personalized product suggestions as well as predictive inventory management. Nevertheless, the same mechanisms

[10] *Ibid*.
[11] *Ibid*.
[12] *Ibid*.

present issues of unfair pricing, no transparency, and manipulation of the consumer behaviour by the use of nudging and behavioural targeting[13].

3.4 CUSTOMER SERVICE AND VIRTUAL ASSISTANTS.

Chatbots and voice assistants (e.g., Alexa, Siri, customer service bots) that operate off AI are becoming more and more involved in consumer-business interaction. The services that they provide include 24/7 support, quicker query resolution, and personalized services. However, there is the risk of misguided advice, lack of accountability and the dehumanization of the redressal process of grievances with reliance on automated systems. Lack of proper oversight mechanisms exposes the consumers to uncertainties in case of the malfunctioning of the AI systems or the presentation of misleading information by the AI.

3. CONSUMER RIGHTS IN DIGITAL ECONOMY

Consumer protection in the digital economy entails safeguarding individuals from information asymmetry, manipulation, and privacy violations caused by widespread data collecting and algorithmic decision-making. The challenges include obtaining meaningful consent for data use, controlling personal information, fair AI-driven pricing, and remedies against algorithmic faults or biased outcomes. Manipulative methods, such as tailored advertising and dark patterns, can jeopardize consumer autonomy and decision-making. Deepfakes and AI-generated material pose risks of fraud and identity misuse[14].

The fundamental Consumer Rights in the Digital Economy.

Right to Safety: Defence against faulty digital items, program bugs, and damages brought about by automated decisions, or algorithm snarls, e.g., biased AI results or security flaws[15].

Right to Information: The right to access transparent, correct and understandable information on products, services, and AI participation, including information on data use and algorithmic decision-making disclosed[16][17].

[13] *Ibid*.
[14] *Ibid*.
[15] *Ibid*.
[16] *Ibid*.
[17] SOCIAL WELFARE, https://socialwelfare.vikaspedia.in/viewcontent/social-welfare/social-awareness/consumer-education/consumer-rights-and-responsibilities?lgn=en (last visited on 8 September, 2025)

Right to Choice: Fair market competition and real choice, without misleading digital marketing strategies such as dark patterns and manipulative AI personalization[18].

Right to Privacy and Data Protection: The Right to be able to choose whether personal data is collected, processed and shared, secured by an informed consent, data minimization, and regulatory control according to the standards such as GDPR and India DPDP Act[19].

Right to Redressal: Effective complaint mechanisms, dispute resolution mechanisms, compensation mechanisms and AI-specific remedies in the event of damage or unjust results by automated systems[20].

Right to Digital Literacy: Giving consumers the authority to be skilled and knowledgeable to use digital technologies, data rights, and risks posed by AI and online applications[21].

3.1 ISSUES AND PROBLEMS.

The digital economy also brings out complexities that include:

- There is inadequate algorithmic transparency, which means that consumers have a difficulty in comprehending AI decisions that affect them[22].
- Transactions across borders make it difficult to enforce consumer rights because of the jurisdictional fragmentation.
- Data-based business models are based on widespread surveillance and profiling, which cause inherent conflict with privacy rights and autonomy.
- The use of AI-based targeted advertising and behavioural nudging in the form of new manipulations of consumers, capitalizes on information asymmetries.

3.2 SIGNIFICANCE OF STRONG LAW AND POLICY REGIMES.

In order to safeguard consumers, the regulations of the digital economy should:

[18] *Ibid*.
[19] *Ibid*.
[20] *Ibid*.
[21] *Ibid*.
[22] *Ibid*.

- Include AI-related specifications on fairness, transparency and accountability.
- Strengthen data protection regulations that guarantee privacy of the consumer of personal details[23].
- Create consumer educational programs that are specialized to encourage digital literacy.
- Empower dispute resolution processes of digital and AI-based harms[24].

Overall, consumer rights within the digital economy are essential to granting trust, equity, and empowerment in more and more AI-mediated markets.

The issue with AI technologies is that they have troubles that traditional consumer law cannot adequately address. These include:

- **Opacity ("black box" algorithms):** Consumer-related decisions are not always transparent, and people cannot interpret and question the results[25].
- **Personalized and dynamic targeting**: AI enables companies to customize products, prices, and marketing at a personal level- which can cause unfair discrimination or manipulation[26].
- **Mass data surveillance:** AI relies on large amounts of consumer data, creating concerns about privacy and consent that were not previously considered in the same way by traditional rules[27].
- **Real time, automated transactions:** A traditional law might have no sufficient solution to the mistakes, prejudice or damage caused by automated systems used on scale and velocity[28].

[23] *Ibid*.
[24] *Ibid*.
[25] *Ibid*.
[26] *Ibid*.
[27] *Ibid*.
[28] *Ibid*.

- **Unwarranted risks (deepfakes, identity theft):** AI-generated content can be utilized to defraud or misuse in a legal context that is more difficult than the usual business[29].

With AI constantly infiltrating everyday consumer behaviour, legal and regulatory frameworks need to adapt swiftly to protect consumer interests and encourage trust within the digital market[30].

4. THEORETICAL FRAMEWORK

The landscape of consumer protection has to be analysed through a strong theoretical framework that would examine how Artificial Intelligence (AI) transforms the notion of consumer protection. The paper is based on three interdependent theories including consumer rights theory, technology law and ethics, and the risk society theory.

4.1 CONSUMER RIGHTS THEORY

Consumer protection is based on the acknowledgment of a number of fundamental consumer rights, first proclaimed by President John F. Kennedy in 1962 and updated by the United Nations Guidelines on Consumer Protection (1985, revised 2015). The rights identified above, right to safety, right to information, right to choose, right to redressal (hearing) and right to privacy, are a source of normative reference point regarding fairness in market dealings.

In this theory, some of the basic consumer safeguards comprise:

- **Right to Safety**: This right allows one to be safeguarded against dangerous products and services which can cause injuries or damage to assets[31].

- **Right to Information**: The right to access correct, complete and transparent information in order to make informed decisions[32].

- **Right to Choice**: Bestowal of diversity and market rivalry[33].

[29] *Ibid*.
[30] *Ibid*.
[31] DEPARTMENT OF CONSUMER AFFAIRS, https://consumeraffairs.gov.in/pages/consumer-rights (last visited on 8 September, 2025)
[32] *Ibid*.
[33] *Ibid*.

- **Right to Redressal:** The right to recover or claim damages on grounds of wrong or unfair trade[34].

- **Right to Privacy:** Management of personal information and avoidance of abuse, which is particularly important in online markets[35].

These liberties form the basis of the consumer empowerment and protection in relation to the AI-mediated market transactions and data flow[36].

4.2 TECHNOLOGY LAW & ETHICS

The crossroads of technology and ethics is an indispensable tool to examine the issue of Artificial Intelligence (AI) in consumer protection. Whereas consumer rights theory focuses on the what of consumer rights, technology law and ethics focus on the how, principles and regulatory mechanisms that are necessary to assure AI responsibility[37].

a) Legal Foundations

Technology law encompasses the set of regulations and laws that attempt to control the digital technologies, such as data protection regulations, e-commerce legislation, and new AI-specific laws. In AI, the conventional rules of the laws of contract, tort law and consumer law face unprecedented challenges. To take an example, consent, at the heart of privacy law, is meaningless in an AI-driven world, where data is in the air and invisible. Equally, liability in the tort law is not clear when the harm is inflicted by autonomous systems as opposed to human beings.

International law tools are slowly rising to these issues. The AI Act (2024) by the European Union contemplates a risk-based regulation model, with the stricter rules towards the high-risk AI systems, such as the consumer-facing applications such as credit scoring. Transparency, accountability, and human oversight are set as guiding principles in the OECD Principles on AI (2019) and G20 AI Guidelines. Although these tools are not universal across the globe, they prove the acknowledgment of the disruptive nature of AI by the legal community.

[34] *Ibid*.
[35] *Ibid*.
[36] *Ibid*.
[37] *Ibid*.

b) Ethical Principles

The principles of legal compliance are not the basis of ethical frameworks of AI governance. Only the most popular are:

- **Equality:** With AI systems, fairness can be guaranteed by making sure that they do not reproduce or enhance biases, which would safeguard customers against discriminatory results.

- **Transparency and Explainability:** Enhancing algorithmic decision-making to be clear, so that consumers may be informed about the way their data is utilized and how decisions are reached.

- **Accountability:** It is necessary to develop mechanisms by which developers, corporations, or regulators should be made accountable to AI-driven harm.

- **Non-Maleficence (Do No Harm):** The avoidance of consumer exploitation by manipulative tactics, e.g. dark patterns or hyper-targeting.

- **Human-Centric Design:** Making sure that AI is used in the service of consumers and not a threat to autonomy or safety.

Organisations such as UNESCO (Recommendation on the Ethics of AI, 2021) and IEEE Global Initiative on Ethically Aligned design have emphasised that ethical AI is not a choice but a precondition to sustainable technological development.

c) Consumer Protection Application.

Technology law and ethics are used in tandem when it comes to the consumer protection against the misuse of AI. The concept of algorithmic fairness, e.g., can be used to combat discrimination in loan approvals; transparency and explainability relate to the right to information; accountability is directly linked to redressal; and the concept of non-maleficence to the right to safety. Ethics therefore fills the gap between the law and what is expected of society, so that AI innovation can be in line with consumer trust and dignity.

4.3 RISK SOCIETY THEORY (ULRICH BECK)

The idea expressed by Ulrich Beck about the risk society applies much to AI. Another aspect of modern societies described in this theory is the spread of wealth in the society as well as the spread of risks that technological progress creates. This is the dynamic of AI. On the one hand, it is efficient and personalized, but on the other, AI poses systemic risks including mass surveillance, discriminatory profiling, and creation of algorithmic control of consumer behaviour. The risk society prism highlights that such risks tend to be global, invisible and hard to control and require novel types of law and institutionalization.

Conceptualized Risk society theory Risk society theory is a theory of modernity that creates new, and frequently systemic risks that individuals cannot contain, which society must control:

- This is illustrated by AI creating so-called manufactured uncertainties- multifaceted, systemic risks in technology, which complicate governance and regulation[38].
- Beck describes the combination of benefits and risks in the technological advancement like the loss of privacy, algorithm injustice, and the threat of automation, which requires new institutions and mechanisms of trust[39][40][41].
- The theory highlights social anxieties and the necessity of making a collective bargain concerning AI risks, with special focus on varied vulnerabilities among social groups[42].
- This prism underscores the wider social-political background of AI consumer protection than instantaneous legal redress[43].

These frameworks collectively provide a clear basis of analysing, designing, and regulating AI-related consumer protection in terms of rights, ethics and managing societal risks[44].

[38] Taberez Ahmed Neyazi, Mitchell Hobbs, Sheryl Wei Ting Ng and Audrey Yue, *Understanding user interactions and perceptions of AI risk in Singapore*, ORIGINAL RESEARCH ARTICLE 1-13 (2023)
[39] *Ibid*.
[40] https://www.slideshare.net/slideshow/ulrich-beck-theory-of-risky-world-technoculture-risk/267152375 (last visited on 8 September, 2025)
[41] Fatih Baş, Artificial Intelligence, *Human and Society in the Context of Ulrich Beck's Risk Society Theory*, JOURNAL OF ESKIŞEHIR OSMANGAZI UNIVERSITY FACULTY OF THEOLOGY 43-59 (2025)
[42] *Ibid*.
[43] *Ibid*.
[44] *Ibid*.

5. LEGAL CHALLENGES IN CONSUMER PROTECTION UNDER AI

AI poses a variety of legal issues for consumer protection that go beyond traditional frameworks, including algorithmic opacity and prejudice, data privacy vulnerabilities, manipulative marketing, liability quandaries, and cross-border regulatory gaps[45][46][47][48][49].

5.1 Algorithmic Opacity & Bias:

AI systems frequently operate as "black boxes," making it impossible to understand how automated judgments are made. This opacity limits consumers' capacity to contest unfair or discriminatory outcomes, particularly when algorithms perpetuate biases encoded in training data. A lack of openness in algorithmic processes leads to outcomes that may disfavour specific groups, hurting fairness and consumer trust[50][51][52][53].

5.2 Data Privacy & Surveillance

AI uses large volumes of personal data, which makes the issue of consumer privacy and informed consent an issue. Brokerage, aggregation, and commercialization of consumer information by platforms is usually done in the absence of significant disclosure, resulting in shadowy digital surveillance. This does not only violate the consumer privacy expectations, but also poses the dangers of identity theft, behavioural profiling and unauthorized data sharing. Current data protection laws, including the GDPR in Europe, endeavour to, but do not consistently, deal with such issues, especially jurisdictional.

The use of AI systems to collect, process, and analyse personal data is rife, often without proper

[45] OVIC, https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/ (last visited on 6, September, 2025)
[46] DENTONS, https://www.dentons.com/en/insights/articles/2025/july/14/challenges-in-establishing-liability-for-ai-driven-products (last visited on 6, September, 2025)
[47] FORTRA, https://dataclassification.fortra.com/blog/ai-data-privacy-challenges-and-solutions (last visited on 6 September, 2025)
[48] CALIFORNIA LAW REVIEW, https://www.californialawreview.org/print/data-privacy-human-rights-and-algorithmic-opacity (last visited on 6 September, 2025)
[49] *Ibid*.
[50] PMC NCBI, https://pmc.ncbi.nlm.nih.gov/articles/PMC8830968/ (last visited on 6 September, 2025)
[51] IBM, https://www.ibm.com/think/topics/algorithmic-bias (last visited on 6 September, 2025)
[52] Keon young Park & Ho Young Yoon, *AI algorithm transparency, pipelines for trust not prisms: mitigating general negative attitudes and enhancing trust toward AI*, 12 HUMANITIES AND SOCIAL SCIENCES COMMUNICATIONS, (2025)
[53] Nil Kumar, Prof. Manoj Dayal, AI-Powered Marketing: A Content Analysis of Bias, Transparency, and Consumer Trust, 4 International Journal of Contemporary Research in Multidisciplinary 146-151, (2025)

consumer awareness or informed consent. Automated data profiling and surveillance subject data to risks of invasion of privacy, unauthorized data sharing, and exposure to security breaches. With many AI models, they need large datasets, meaning they will over-collect more than is needed, in ways that consumers cannot fully control or comprehend. Additional complexity to consumer protection is the cross-jurisdictional disparities in privacy laws[54][55][56].

5.3 Manipulative Marketing

AI allows hyper-targeted advertising on the basis of predictive analytics of consumer behaviour. On the one hand, personalization will lead to consumer choice improvement, but on the other hand, there is a risk of going beyond it into the sphere of manipulation by taking advantage of cognitive biases and emotional weaknesses. These practices negatively affect consumer autonomy and confuse the process of persuasion with the one of coercion. Conventional consumer protection regimes, based on the misleading or unfair practice, are poorly placed to govern these dark patterns and algorithmic nudges.

Hyper-targeted advertising has led to firms using AI to capitalize on personal information and psychological weaknesses in order to develop highly personalized marketing aimed at nudging or manipulating the consumer decision-making process. This kills consumer discretion and could blur the distinction between persuasion and exploitation. Behavioural advertising driven by AI is employed on many platforms with the aim of maximizing profit, rather than consumer welfare[57][58][59].

5.4 Liability Dilemmas

It is also challenging to define legal responsibility in regards to harms caused by AI-driven products. Whether the person who created the algorithm, or the platform it is on, or the seller utilizing it is responsible for its negative effects may be ambiguous, particularly in the autonomous and developing nature of AI. The new EU legislation is very strict on product

[54] *Ibid*.
[55] DATA GUARD, https://www.dataguard.com/blog/growing-data-privacy-concerns-ai/ (last visited on 6 September, 2025)
[56] THE LEGAL SCHOOL, https://thelegalschool.in/blog/ai-and-data-privacy (last visited on 6 September, 2025)
[57] Harinder Hari, Arun Sharma, Sanjeev Verma, Rijul Chaturvedi, *Exploring ethical frontiers of artificial intelligence in marketing*, 21 JOURNAL OF RESPONSIBLE TECHNOLOGY 1-13, (2025)
[58] FORBES, https://www.forbes.com/sites/elijahclark/2024/03/14/the-ethical-dilemma-of-ai-in-marketing-a-slippery-slope/ (last visited on 6 September, 2025)
[59] *Ibid*.

liability in particular situations but there are still issues to overcome on the demonstration of causality or defect with autonomous systems. The absence of accountability makes consumers more vulnerable[60].

5.5 Cross-border Issues

AI-powered platforms and services operate on a global scale, making it challenging to implement consumer protection consistently across states. Differing privacy, security, and liability requirements among countries create loopholes that impede consumer redress and regulatory supervision. Data transfers and algorithmic judgments that span national borders hamper the implementation of local consumer law[61].

Overall, legal systems around the world are failing to keep up with these issues, which require new approaches to transparency, accountability, and consumer rights in the age of artificial intelligence[62].

6. CURRENT LEGAL & REGULATORY FRAMEWORKS

6.1 INDIA- CONSUMER PROTECTION ACT 2019, IT ACT, DATA PROTECTION LAW (DPDP ACT 2023).

Current legal and regulatory frameworks addressing AI-driven consumer protection encompass comprehensive statutes in India and internationally, but face developing issues in the context of algorithmic decision-making, personal data, liability, and cross-border enforcement [63] [64] [65] [66] [67] [68] [69].

---

[60] *Ibid*.
[61] *Ibid*.
[62] *Ibid*.
[63] IRIS LAW, https://erislaw.se/artiklar/the-eus-double-edged-sword-balancing-innovation-with-consumer-protection-in-the-ai-age/ (last visited on 6 September, 2025)
[64] *Ibid*.
[65] https://www.beuc.eu/sites/default/files/publications/BEUC-X-2022-136_The_limits_of_the_AI_Act_and_why_consumers_need_better_protection.pdf (last visited on 6 September, 2025)
[66] ANSI, https://www.ansi.org/standards-news/all-news/5-9-24-oecd-updates-ai-principles (last visited on 6 September, 2025)
[67] INTERNATIONAL TRADEMARK ASSOCIATION, https://www.inta.org/perspectives/features/how-the-eu-ai-act-supplements-gdpr-in-the-protection-of-personal-data/ (last visited on 6 September, 2025)
[68] IAPP, https://iapp.org/news/a/consumer-protection-in-the-age-of-ai-the-ftcs-approach-to-ai-regulation (last visited on 6 September, 2025)
[69] FUTURE OF PRIVACY FORUM, https://fpf.org/blog/five-ways-in-which-the-dpdpa-could-shape-the-development-of-ai-in-india/ (last visited on 6 September, 2025)

India: Key Legislations

- The Consumer Protection Act of 2019 improved consumer rights by increasing definitions and providing remedies for unfair commercial practices in the digital economy, such as deceptive ads and e-commerce abuses. AI-enabled goods may be subject to product responsibility provisions, which hold manufacturers, service providers, and dealers responsible for any harm caused[70][71][72].

- The IT Act of 2000 and its amendments regulate digital transactions, cybercrime, and intermediary liability, but have limited, indirect application to AI-related harms.

- The Digital Personal Data Protection Act (DPDP) 2023 offers comprehensive data protection rights, with a focus on lawful processing, consent, right to access/erasure, and regulatory supervision. However, explicit AI-specific rights are still being developed, such as the "Right to be Forgotten" in AI contexts[73][74].

6.2 INTERNATIONAL – EU'S AI ACT, GDPR, OECD GUIDELINES, US APPROACH.

a) European Union

The EU AI Act (2024) represents a pioneering regulatory framework that adopts a risk-based approach to ensure the trustworthiness of artificial intelligence systems. It mandates stringent requirements for transparency, accountability, and human oversight, with a particular emphasis on high-risk systems[75]. This framework is enforced by national authorities and is complemented by the General Data Protection Regulation (GDPR), which establishes robust rules concerning fairness, consent, transparency, data minimization, and individual rights in data processing. These rules are directly applicable to the training and deployment of AI models

[70] Shatakshi Johri, *Emerging artificial intelligence and its cascading effects on consumer protection in India: An analytical study*, 19 WORLD JOURNAL OF ADVANCED RESEARCH AND REVIEWS 1554-1558, (2023)
[71] Dr. Priya Roy, Rituraj Bhowal, *An Analysis of Product Liability for AI Entities with special reference to the Consumer Protection Act, 2019,* 17 THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW, (2022)
[72] LAW SCHOOL POLICY REVIEW, https://lawschoolpolicyreview.com/2025/02/12/addressing-product-and-service-liability-concerns-in-artificial-intelligence-an-indian-perspective/ (last visited on 6 September, 2025)
[73] EY, https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023 (last visited on 6 September, 2025)
[74] *Ibid*.
[75] *Ibid*.

utilizing personal data[76]. Additionally, the Product Liability Directive (2024) extends the definition of "product" to encompass digital and AI-powered services, thereby enabling strict liability for defects and simplifying the processes for consumer claims[77].

b) OECD Guidelines

The OECD AI Principles, updated in 2024, emphasize the necessity for AI systems to be trustworthy, transparent, accountable, and human-centric, establishing global standards for policymakers and industry stakeholders[78][79].

c) United States

There is no overarching federal statute specifically governing AI; instead, sector-specific laws such as the FTC Act, COPPA, and FCRA address issues related to deceptive practices, privacy, and discrimination within AI contexts. Agencies like the FTC utilize their existing authority to ensure consumer protection in AI applications. Notably, Colorado's AI Act, enacted in 2026, represents the first state-level legislation imposing specific obligations on developers and deployers of high-risk AI systems[80][81].

6.3 Judicial perspectives

- Indian courts have begun to engage with AI-related issues in consumer disputes and broader digital rights, although doctrinal development remains in progress. While explicit judgments on AI liability are limited, there is a discernible trend of judicial concern regarding transparency, fairness, and the right to effective redress[82][83].

- In the European Union, courts and regulators have acknowledged AI-related harms,

[76] *Ibid*.
[77] *Ibid*.
[78] *Ibid*.
[79] AI EHTICS LAB, https://aiethicslab.rutgers.edu/glossary/oecd-ai-principles/ (last visited on 6 September, 2025)
[80] *Ibid*.
[81] MOFO, https://www.mofo.com/resources/insights/240531-navigating-new-frontiers-colorado-s-groundbreaking-ai (last visited on 7 September, 2025)
[82] Rajesh Bahuguna & Radhey Shyam Jha, *Age-old tools and techniques to protect consumers age-old tools and techniques to Protect Consumers need to be sharpened in the light of Artificial Intelligence*, 10 INTERNATIONAL JOURNAL ON CONSUMER LAW AND PRACTICE INTERNATIONAL JOURNAL ON CONSUMER LAW AND PRACTICE 81-98 (2022)
[83] SSRANA, https://ssrana.in/articles/supreme-courts-guidance-on-the-use-of-generative-ai-tools-in-court-proceedings/ (last visited on 7 September, 2025)

particularly in relation to GDPR breaches, liability, and rights to explanation and rectification. Landmark cases have significantly influenced the interpretation of these issues by Member States[8485].

- In the United States, the Rite Aid case, adjudicated by the FTC, serves as a notable example of agency enforcement against opacity and discrimination in AI-driven consumer contexts[86].

These regulatory frameworks are continually evolving to address the rapid advancements in AI technology and emerging consumer vulnerabilities, with an expanded focus on robust enforcement, international harmonization, and the implementation of practical safeguards to protect rights within the digital marketplace[87].

7. CASE STUDIES OF AI-DRIVEN CONSUMER HARMS

Although a lot of this debate on Artificial Intelligence and consumer protection is merely speculative, there are concrete examples of how AI-mediated markets pose a real danger to consumers. These examples bring out the fact that current consumer protection regulations do not always work as well when it comes to algorithmic harms.

7.1 Prejudiced Loan Grants- Apple Card (2019)

In 2019, the credit card offered by Apple in collaboration with Goldman Sachs was put under investigation after consumers have complained that the algorithm will constantly give women lower credit limits than men with the same financial background. That prompted the concerns of algorithmic bias in financial decisions where consumers could not see much of what was going on behind the curtain of determining their creditworthiness. The case brought attention to a noticeable loophole in regulation: the traditional anti-discrimination regulations failed to

[84] *Ibid*.
[85] TECHGDPR, https://techgdpr.com/blog/ai-and-the-gdpr-understanding-the-foundations-of-compliance/ (last visited on 7 September, 2025)
[86] *Ibid*.
[87] *Ibid*.

sufficiently address the black-box AI systems in the consumer finance[88][89][90][91].

7.2 Manipulative Design - Amazon Dark Patterns (2021-2023)

Both American and European regulators discovered that Amazon applied AI-optimized dark patterns in which consumers found it artificially hard to cancel Prime subscriptions. The design played the consumer psychology game, and it was subtly pushing the users to continue subscribing when they did not want to. This case illustrates that AI can persuade the consumer to lose their autonomy without drawing much attention, which leads to ethical concerns regarding unfair trade practices. Although enforcement action has been applied, the law had to adapt the conventional meaning of misleading and unfairness practices to apply to algorithmic manipulation[92].

7.3 Scam Cambridge Analytica Scandal (2018).

The Cambridge Analytica scandal demonstrated that the Facebook data of millions of people was being mined and processed using AI software to form psychographic profiles to be used in micro-targeted political advertising. Even though it is more of a data protection problem, the incident showed how the concept of algorithmic profiling may jeopardize consumer privacy and the validity of choice since people were manipulated without their knowledge. It highlighted the weaknesses of the consent-based models to control data-driven AI systems[93].

7.4 Algorithms Pricing - Travel Agencies.

Research on travel booking websites found that the pricing was dynamically changed by algorithm, with or without charging users more due to their device (e.g. Apple users) or returning search results repeatedly. Although strictly speaking a type of personalized pricing, this practice was a blurring of the business strategy and exploitation of the consumers, with consumers not being aware of the algorithm processes that go behind the scenes to determine

[88] BBC, https://www.bbc.com/news/business (last visited on 8 September, 2025)
[89] THE VERGE, https://www.theverge.com/2019/11/11/20958953/apple-credit-card-gender-discrimination-algorithms-black-box-investigation (last visited on 8 September, 2025)
[90] TECH CRUNCH, https://techcrunch.com/2022/07/01/amazon-ends-prime-cancellation-dark-patterns-europe/ (last visited on 8 September, 2025)
[91] CNBC, https://www.cnbc.com/2019/11/11/goldman-sachs-to-reevaluate-apple-card-credit-limits-after-bias-claim. (last visited on 8 September, 2025)
[92] *Ibid*.
[93] WIKIPEDIA, https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal (last visited on 8 September, 2025)

the prices that they pay. Conventionally defined consumer protection legislation failed to foresee this form of AI-based price discrimination.

7.5 The AI Misinformation - Chatbots in healthcare.

In some instances, AI-based medical chatbots have given wrong or false medical information, such as minimizing the symptoms of a severe illness. The injury, in contrast to that of defective goods, is that of allegation hallucinations generated by the algorithm, which presents new questions on product liability and the duty of care. Even with no definite criteria on AI safety in health services that address consumers, consumers are exposed when they use such systems[94].

8. REGULATORY GAPS AND CHALLENGES

Traditional consumer protection laws are increasingly inadequate to tackle the harms resulting from AI, due to the opacity inherent in algorithms, the complexity of enforcement, and the tension between encouraging innovation and safeguarding consumer rights, which combined produce vast regulatory gaps and challenges[9596].

1. Inadequacy of Traditional Laws

Most laws were written prior to the popularization of AI and are inadequate to address the dangers of automated data-driven systems. Key issues include no explicit provisions for algorithmic discrimination, misuse of data and manipulative digital practices. For example, product liability laws are ill-suited to address harm caused by autonomous "black box" models, and many consumer data rights are not completely compatible with AI's ongoing, adaptive use of data. There is confusion in the definition of liability and causation of harms regarding complex and developing AI systems[9798].

---

[94] VERY WELL HEALTH, https://www.verywellhealth.com/why-you-should-never-use-chatgpt-for-health-advice (last visited on 8 September, 2025)

[95] Ruchi Agarwal, The Role of AI in Consumer Protection Act in Current Scenario https://www.lawctopus.com/academike/the-role-of-ai-in-consumer-protection-act-in-current-scenario/ (last visited September 7, 2025)

[96] *Ibid*.

[97] *Ibid*.

[98] LAW FARE MEDIA, https://www.lawfaremedia.org/article/are-existing-consumer-protections-enough-for-ai (last visited on 7 September, 2025)

2. Enforcement Difficulties: Black-Box AI

The opaque nature of most AI systems-algorithms are black boxes and therefore it is incredibly hard for regulators, courts, or even consumers to understand and appeal decisions, detect biases, or audit results[99]. The absence of transparency hinders proving a wrong or harm, and creates gaps in redressing the consumer. Audit trails and explainable AI are being developed as potential solutions, but they are still incomplete and difficult to use in dynamic, learning systems[100101102103].

3. Balancing Innovation and Consumer Rights

One of the foundational issues of regulation is how to allow responsible technological innovation without putting consumers at unnecessary risk. Excessively stringent, unclear, or disjointed regulation may hinder positive AI development and prevent market competition. In contrast, under-regulation exposes consumers to discrimination, manipulation, and a loss of autonomy. Jurisdictions such as the EU are attempting to address this through risk-based frameworks and liability reforms, but politicians continue to grapple with how dynamic AI is and how to best provide consumer protection while promoting growth[104105106107].

To preserve consumer safety and trust while encouraging innovation, the global regulatory landscape calls for clearer, AI-tailored regulations, practical enforcement measures, and continuing communication[108109].

---

[99] EW SOLUTION, https://www.ewsolutions.com/understanding-black-box-ai/ (last visited on 7 September, 2025)
[100] *Ibid*.
[101] GILBRATAR, https://gibraltarsolutions.com/blog/navigating-the-ai-black-box-problem/ (last visited on 7 September, 2025)
[102] AI COMPETENCE, https://aicompetence.org/audit-trails-for-black-box-ai/ (last visited on 7 September, 2025)
[103] FINANCE WATCH, https://www.finance-watch.org/policy-portal/digital-finance/protecting-eu-consumers-in-the-age-of-ai-driven-retail-finance/ (last visited on 7 September, 2025)
[104] Vijaya Venkata Sri Rama Bhaskar, Akhil Mittal, Santosh Palavesh, Krishnateja Shiva, Pradeep Etikani, Regulating AI in Fintech: Balancing Innovation with Consumer Protection, 10 European Economic Letters 78-86 (2020),
[105] *Ibid*.
[106] INSURANCE THOUGHT LEADERSHIP, https://www.insurancethoughtleadership.com/regulation-public-policy/balancing-ai-innovation-consumer-protection (last visited on 7 September, 2025)
[107] AI SIGIL, https://aisigil.com/ai-regulation-balancing-innovation-and-consumer-protection/ (last visited on 7 September, 2025)
[108] *Ibid*.
[109] *Ibid*.

9. PROPOSED REGULATORY RESPONSES

To effectively address the challenges posed by Artificial Intelligence (AI) in consumer markets, regulatory responses must transcend traditional consumer protection models and adapt to the complexities inherent in algorithm-driven commerce. Effective regulation should be multidimensional, encompassing transparency, accountability, redressal, cross-border enforcement, and consumer empowerment. The following measures are particularly significant:

1. Algorithmic Transparency and Explainability Mandates

It is imperative that both consumers and regulators comprehend the decision-making processes of AI systems. Mandating algorithmic transparency and explainability would mitigate the risks associated with "black box" harms by obligating companies to disclose key factors influencing automated outcomes. Such mandates could be enforced through regulatory audits, disclosure requirements, and impact assessments. The European Union’s proposed AI Act already emphasizes explainability in high-risk AI systems, a model that jurisdictions such as India could adapt within their consumer protection and data governance frameworks.

2. Standards for Fairness, Accountability, and Ethical AI

AI regulation must integrate ethical principles into legal standards to safeguard consumer interests. This includes embedding fairness (avoiding discriminatory outcomes), accountability (assigning liability to specific actors in the AI supply chain), and responsibility (ensuring compliance through monitoring and penalties). Industry-wide codes of conduct and legally enforceable standards could require businesses to conduct algorithmic impact assessments and adopt bias-mitigation practices. Independent oversight bodies, akin to data protection authorities under GDPR, could ensure compliance.

3. Strengthening Consumer Redressal Mechanisms

Traditional consumer redressal forums may not be adequately equipped to handle disputes involving AI. Mechanisms should be updated to include specialized digital consumer courts or ombudsmen capable of addressing algorithmic harms. Online dispute resolution (ODR) systems can provide quicker remedies for cross-platform issues. Importantly, liability rules

must be clarified to assign responsibility among developers, service providers, and sellers, ensuring that consumers are not left without recourse when AI-driven harm occurs.

4. Cross-Border Cooperation and Harmonization of AI Regulations

Given that AI-enabled platforms operate globally, fragmented regulatory regimes weaken consumer protection. Cross-border cooperation through treaties, international guidelines (such as the OECD AI Principles), and mutual recognition of standards would facilitate the harmonization of regulations. For instance, disputes involving multinational e-commerce platforms could be addressed through international arbitration mechanisms or consumer protection frameworks coordinated at the WTO or UNCTAD level. Without such harmonization, jurisdictional conflicts will continue to leave consumers unprotected.

5. Role of Consumer Awareness and Digital Literacy

Regulatory frameworks must also acknowledge the importance of empowering consumers. Awareness campaigns and digital literacy programs can equip consumers with the skills to recognize manipulative marketing, protect personal data, and exercise their rights under AI-driven systems. Educational initiatives should emphasize informed consent, safe online behaviour, and mechanisms for grievance redressal. A well-informed consumer base acts as the first line of defence against exploitative practices, complementing formal regulation.

10. CONCLUSION

Artificial Intelligence (AI) has emerged as a transformative force within consumer markets, fundamentally altering the manner in which goods and services are advertised, delivered, and experienced. While its integration offers undeniable advantages in terms of efficiency, personalization, and innovation, it concurrently introduces unprecedented risks that traditional consumer protection laws were not designed to address. Issues such as algorithmic opacity, data-driven manipulation, privacy violations, liability dilemmas, and cross-border complexities collectively create a regulatory vacuum, leaving consumers vulnerable.

The analysis underscores that existing frameworks, including India's Consumer Protection Act, 2019, the Digital Personal Data Protection Act, 2023, and international models such as the EU GDPR and AI Act, provide valuable foundations but remain inadequate in addressing the full spectrum of AI-driven harms. The enforcement challenges posed by "black box" systems,

coupled with the tension between fostering innovation and safeguarding rights, highlight the urgent need for legal reform.

To advance, consumer protection in the AI era must be based on a hybrid model that integrates legal, ethical, and technological safeguards. This includes mandating algorithmic transparency and explainability, establishing enforceable standards of fairness and accountability, strengthening consumer redressal forums, harmonizing cross-border regulations, and investing in digital literacy. Such a multidimensional approach would not only ensure effective protection of consumer rights but also build public trust in AI technologies, which is crucial for their sustainable adoption.

Ultimately, the objective is not to resist technological change but to guide it responsibly to ensure that innovation serves consumers rather than exploits them. By proactively addressing regulatory gaps and aligning AI deployment with principles of justice, fairness, and accountability, policymakers can create a consumer protection regime that is future-ready, equitable, and resilient in the age of Artificial Intelligence.