Page: 309-327 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume IV | Special Issue I

2026

Special Issue on the International E-Conference on

"Law in the Age of Artificial Intelligence: A Fundamental Perspective"

Organised by KES' Shri J. H. Patel College of Law, Mumbai, on 24 January 2026

Official Publication Partner: LawFoyer International Journal of Doctrinal Legal Research

DOI: https://doi.org/10.70183/lijdlr.2026.v4si1.19

KES' Shri. Jayantilal H. Patel Law College

About the College

KES' Shri. Jayantilal H. Patel Law College is committed to nurturing and empowering students through quality legal education. The college provides an inclusive and academically enriching environment that encourages students to excel in their studies, participate in co-curricular activities, engage in research, and develop a strong sense of civic responsibility.

The college is affiliated to the University of Mumbai, approved by the Bar Council of India, NAAC accredited with 'B++' grade, and ISO 9001:2015 certified. It offers programmes including B.A. LL.B., LL.B., LL.M., and specialised diploma courses.

With qualified and experienced faculty, a strong academic environment, moot court training, research activities and modern infrastructure, the institution seeks to prepare responsible, skilled and socially conscious legal professionals equipped to meet the challenges of a rapidly changing world.

The college functions under the aegis of Kandivli Education Society (KES), an institution established in 1936 with a long-standing commitment to quality, inclusivity and value-based education.

Affiliation	University of Mumbai
Recognition	Approved by the Bar Council of India
Accreditation	NAAC accredited 'B++'
Certification	ISO 9001:2015 certified

Kandivli Education Society

Established 1936

Kandivli Education Society (KES), established in 1936, has grown from a small educational initiative into a dynamic educational institution serving thousands of students.

With a legacy of quality, inclusivity and value-based learning, KES has expanded its academic presence across various disciplines. Its educational institutions are committed to providing meaningful learning opportunities and fostering academic, professional and personal development among students.

KES' Shri. Jayantilal H. Patel Law College is one of its prominent institutions dedicated to legal education. Through academic excellence, research, practical learning and co-curricular engagement, the college seeks to empower students with the knowledge, skills and values necessary to contribute meaningfully to society.

Educational Commitment

- Quality and inclusive education
- Value-based learning
- Academic and professional development
- Research and practical learning
- Holistic and future-ready education

Law in the Age of Artificial Intelligence

A Fundamental Perspective

About the International Conference

The International Conference on "Law in the Age of Artificial Intelligence: A Fundamental Perspective" provided an academic platform to examine the transformative impact of Artificial Intelligence on law, legal systems, governance and society.

The conference explored emerging legal and ethical questions relating to Artificial Intelligence, including intellectual property, authorship and ownership, liability, data privacy, cybersecurity, criminal justice, evidence law, human rights, ethics and accountability. It addressed the implications of Artificial Intelligence for legal education, commercial law, regulatory frameworks, policy development, research and scholarly communication.

The conference brought together academicians, research scholars, legal professionals and students to present research, exchange ideas and engage in interdisciplinary discussions. It encouraged meaningful academic dialogue and contributed towards the development of effective, ethical and inclusive legal responses to the rapidly evolving Artificial Intelligence landscape.

Conference	International Conference
Theme	Law in the Age of Artificial Intelligence: A Fundamental Perspective
Date	24 January 2026
Time	10:00 AM onwards
Mode	Online
Organised by	IQAC, Student Research Society and Library Committee
Publication Partner	LawFoyer International Journal of Doctrinal Legal Research [ISSN: 2583-7753]

Principal's Message

KES' Shri. Jayantilal H. Patel Law College

It gives me immense pleasure to welcome all academicians, research scholars, legal professionals and students to the International Conference on "Law in the Age of Artificial Intelligence: A Fundamental Perspective."

Artificial Intelligence is transforming the way societies function and is increasingly influencing legal systems, governance, professional practices and education. These developments bring significant opportunities as well as complex legal, ethical and social challenges.

This conference provided a valuable platform for intellectual exchange and interdisciplinary dialogue on emerging issues such as data privacy, intellectual property, liability, criminal justice, human rights, ethics and the governance of Artificial Intelligence. The scholarly contributions and discussions during the conference encouraged deeper understanding and promoted responsible approaches to the use of Artificial Intelligence.

I extend my best wishes to all the speakers, researchers, presenters, participants and members of the organising team for a meaningful and intellectually enriching conference.

Dr. Viral Dave
I/c. Principal
KES' Shri. Jayantilal H. Patel Law College

Organising Committee

International Conference on Law in the Age of Artificial Intelligence

I/c. Principal	Dr. Viral Dave
Convenor	Mr. Mahavir Mandot
Co-Convenors	Dr. Shweta Vijendra Pathak Ms. Priyanka Khakhadia Ms. Deepanshi Chandarana

Organised by IQAC, Student Research Society and Library Committee

KES' Shri. Jayantilal H. Patel Law College, Mumbai

Papers presented at the conference are published in the Special Issue of the LawFoyer International Journal of Doctrinal Legal Research [Volume IV, Special Issue I, 2026]

CONSUMER PROTECTION IN THE ERA OF AI-DRIVEN PRODUCTS AND SERVICES

Dr. Deepanshi Dahiya Chandarana[1] & Adv. Harjas Pratap Singh Anand[2]

I. ABSTRACT

Artificial Intelligence (AI) has rapidly transformed the way consumers interact with products and services. From personalized recommendations on e-commerce platforms to AI-powered chatbots, virtual assistants, automated financial services, and smart devices, AI has become deeply embedded in everyday consumer experiences. While these technological advancements offer greater convenience, efficiency, and personalization, they also raise important concerns regarding consumer rights and protection. The increasing reliance on AI-driven systems has given rise to several challenges, including algorithmic bias, lack of transparency in decision-making, misuse of personal data, targeted manipulation of consumer behaviour, and difficulties in determining liability when harm occurs. Traditional consumer protection laws were primarily designed for human-driven transactions and may not adequately address the unique risks posed by autonomous and data-intensive technologies. This paper examines the evolving relationship between artificial intelligence and consumer protection by analysing the legal and regulatory challenges associated with AI-driven products and services. It explores whether existing consumer protection frameworks are capable of safeguarding consumers in an increasingly automated marketplace and evaluates emerging regulatory approaches adopted across different jurisdictions. The paper further highlights the need for greater transparency, accountability, data protection, and effective redress mechanisms to ensure that technological innovation does not come at the cost of consumer rights. Despite growing scholarship on AI governance and data privacy, limited attention has been devoted to examining consumer protection concerns arising specifically from AI-driven products and services. This paper seeks to address this gap by evaluating the adequacy of existing consumer protection frameworks in the context of emerging AI technologies. The study concludes that while AI has the potential to significantly enhance consumer welfare, its responsible deployment requires a robust and

[1] Dr.Deepanshi Dahiya Chandarana,Assistant Professor,KES Shri Jayantilal H. Patel Law College (India).Email: deepanshi.chandarana@gmail.com
[2] Advocate at Delhi High Court (India).Email: harjasanand13@gmail.com

 (ISSN: 2583-7753)

adaptive legal framework that balances innovation with fairness, trust, and consumer protection in the digital age.

II. KEYWORDS

Artificial Intelligence, Consumer Protection, Algorithmic Accountability, Data Privacy, AI Regulation.

III. INTRODUCTION

The rapid development of artificial intelligence (AI) has transformed the manner in which businesses interact with consumers and deliver products and services.[3] AI technologies are increasingly being incorporated into various sectors, including e-commerce, banking, healthcare, insurance, transportation, and digital entertainment.[4]

The expanding use of AI has undoubtedly enhanced efficiency, convenience, and personalisation for consumers.[5] Businesses are now able to analyse consumer behaviour, anticipate preferences, and offer tailored products and services at an unprecedented scale. Consumers, in turn, benefit from faster services, improved accessibility, and more informed purchasing choices. However, alongside these benefits, AI-driven technologies have also given rise to several legal and ethical concerns that challenge conventional notions of consumer protection. One of the primary concerns is the lack of transparency in algorithmic selection.

Consumers are often unaware of how AI systems collect, process, and use their personal data to influence decisions that affect them. Additionally, the growing use of AI in areas such as credit scoring, insurance assessment, dynamic pricing, and targeted marketing raises concerns regarding fairness, accountability, and potential discrimination The potential for algorithmic bias, unlawful discriminatory outcomes, and manipulative digital practices highlights the vulnerability of consumers in an increasingly automated marketplace. Traditional consumer protection laws were developed in an era in which commercial decisions were generally made by identifiable human actors.

---

[3] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed., Pearson 2021

[4] NITI Aayog, *National Strategy for Artificial Intelligence: #AIforAll* (2018).

[5] OECD, *Recommendation of the Council on Artificial Intelligence* (2019)

As a result, many existing legal frameworks struggle to address the complexities associated with autonomous, algorithmic, and data-driven technologies. Questions concerning liability, transparency, consumer consent, and effective redress mechanisms remain inadequately addressed in many jurisdictions. Consequently, there is a growing need to examine whether existing consumer protection regimes are capable of safeguarding consumer interests in the age of artificial intelligence. This paper seeks to analyse the emerging challenges posed by AI-driven products and services from a consumer protection perspective.

It examines the risks associated with algorithmic decision-making, data privacy, and unfair commercial practices, while evaluating the adequacy of existing legal and regulatory frameworks. The paper further examines regulatory developments across different jurisdictions and proposes measures to strengthen consumer protection without unduly hindering technological innovation. By analysing the intersection between artificial intelligence and consumer rights, this study aims to contribute to the ongoing discourse on developing a balanced, accountable, and consumer-centric approach to AI governance.

A. Research Objectives

The increasing integration of Artificial Intelligence into consumer markets has transformed the nature of commercial interactions and service delivery. While AI-driven technologies offer several benefits, they also raise concerns regarding transparency, privacy, fairness, and accountability. In this context, the present study seeks to examine the implications of AI-driven products and services from a consumer protection perspective.

The specific objectives of this research are:

1. To examine the growing role of Artificial Intelligence in consumer products and services.
2. To identify the challenges posed by AI-driven technologies to consumer rights, particularly in relation to transparency, privacy, informed consent, and fairness.

3. To analyse the adequacy of existing consumer protection laws in addressing risks associated with AI-based decision-making systems.
4. To evaluate emerging regulatory approaches adopted by different jurisdictions for governing AI technologies.
5. To propose recommendations for strengthening consumer protection while promoting responsible innovation and technological advancement.

B. Research Methodology

The present study adopts a doctrinal research method based on the analysis of primary and secondary legal sources. The research is primarily based on legal provisions, legal decisions, government reports, policy documents, international guidelines, academic literature and scientific articles related to artificial intelligence and consumer protection.

The study undertakes a qualitative analysis of the existing legal framework governing consumer rights in the context of AI-powered products and services. Special emphasis is placed on examining the Consumer Protection Act, 2019, the Digital Personal Data Protection Act, 2023 (DPDP Act), and relevant international regulatory developments, including the European Union's AI regulatory framework and data protection laws. In addition, the research adopts a comparative approach to understand how different jurisdictions are responding to the challenges posed by artificial intelligence. By examining the legislative process and regulatory efforts across different jurisdictions, the study seeks to identify best practices that can contribute to the development of an effective and user-centric AI governance framework.

The scope of this study is limited to the consumer protection implications of AI-powered products and services and does not extend to broader issues of intellectual property, national security, or criminal liability arising from the use of artificial intelligence technologies.

 (ISSN: 2583-7753)

IV. CONSUMER PROTECTION CHALLENGES IN THE ERA OF AI-DRIVEN PRODUCTS AND SERVICES

Artificial intelligence has fundamentally changed the way companies interact with consumers. With advanced data analytics, machine learning algorithms, and automated decision-making systems, companies can now predict consumer preferences, personalize services, and optimize commercial operations with remarkable efficiency. However, the same technology that enhances user experiences can also create significant risks that challenge traditional consumer protection rules.

Increasing dependence on AI-powered systems has exposed users to a host of concerns regarding transparency, privacy, fairness, accountability, and autonomy. Unlike conventional business practices, where decisions are made by identifiable individuals, AI systems often operate through complex algorithms that remain inaccessible and incomprehensible to ordinary users. As a result, consumers may be negatively affected by decisions without fully understanding the factors that affected them.

A. Lack of Transparency and Explainability

One of the most significant challenges associated with AI-powered products and services is the lack of transparency in algorithmic decision-making. Many AI systems operate as "black boxes," meaning that even programmers can struggle to explain how certain decisions are made.[6]

Consumers increasingly face automated decision-making when applying for credit, buying insurance, receiving product recommendations, or interacting with digital platforms. However, in most cases, they are given little or no information regarding the criteria used by AI systems to arrive at those decisions. This lack of transparency undermines the consumer's ability to make informed choices and to challenge potentially unfair outcomes.

The lack of explainability becomes particularly problematic when AI-generated decisions have significant economic or social consequences. Without adequate

[6] Frank Pasquale, *The Black Box Society* (Harvard University Press 2015)

transparency, users may have difficulty identifying errors, biases, or discriminatory practices embedded in automated systems. Thus, there is a growing demand for legal frameworks that recognize a consumer's right to meaningful explanations regarding important automated decisions affecting them.[7]

B. Algorithmic Bias and Discrimination

Another major concern that arises from implementing AI systems is the potential for algorithmic bias. AI systems are trained using large amounts of historical data. Where such data reflects existing social inequalities or biases, AI systems may inadvertently reproduce and reinforce those biases.[8]

Algorithmic bias can manifest in a variety of forms. For example, automated credit rating systems can harm individuals who belong to certain socioeconomic groups, while AI-powered recruitment tools can show gender or racial bias. Similarly, targeted advertising algorithms can reinforce stereotypes by selectively displaying opportunities or information to specific groups of users.

From a consumer protection perspective, discriminatory results undermine the principles of fairness and equal treatment. The challenge is compounded by the difficulty consumers have in detecting and proving algorithmic discrimination. Because AI systems often operate without transparency, users may be unaware that they have been subjected to biased decision-making processes.

C. Data Privacy and Consumer Surveillance

Data has often been described as the 'new oil' of the digital economy, a phrase widely attributed to Clive Humby in 2006, and Artificial Intelligence systems rely heavily on the collection, processing, and analysis of vast amounts of consumer data. Every online search, purchase, click, location update, and interaction with a digital platform generates valuable information that can be used to train AI systems and predict consumer behaviour. While such data-driven practices allow companies to offer personalised services and improved user experiences, they also raise serious concerns

[7] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," 7(2) International Data Privacy Law 76 (2017)
[8] Cathy O'Neil, *Weapons of Math Destruction* (2016).

regarding consumer privacy, autonomy, and surveillance. One of the primary concerns is that consumers are often unaware of the extent to which their personal data is being collected and processed. Privacy regulations are often lengthy, complex, and difficult to understand, resulting in users giving consent without fully appreciating the consequences of data sharing. Thus, the concept of informed consent, which is the foundation of modern data protection law, is increasingly being challenged in AI-driven environments.

The extensive collection of user data also creates risks of surveillance and profiling. AI systems can develop highly detailed user profiles by analyzing purchasing patterns, browsing histories, social media activity, and even behavioral characteristics. Such profiling allows companies to predict consumer preferences with remarkable accuracy; however, it can also lead to intrusive surveillance and excessive intrusion into an individual's privacy.

In addition, the centralization of large amounts of personal information increases the risk of data breaches and unauthorized access. As AI systems become more sophisticated and interconnected, ensuring the security and responsible use of user data becomes an important part of consumer protection. The challenge for policymakers lies in balancing the benefits of data-driven innovation with the need to preserve privacy, dignity, and individual autonomy.[9]

D. Manipulative Advertising and Dark Patterns

The growing use of AI in digital marketing has significantly changed advertising practices. With advanced analytics and behavioural prediction models, companies can now deliver highly personalized ads tailored to individual user preferences and vulnerabilities. Although personalization can increase consumer convenience, it also raises concerns regarding manipulation and unfair commercial practices.

AI-powered advertising systems are able to analyse vast amounts of consumer data to identify behavioural tendencies, emotional responses, and buying habits. Such information can be used to influence consumer decisions in ways that consumers may not fully recognize. The distinction between persuasion and manipulation is

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

becoming increasingly blurred as companies leverage AI to exploit psychological vulnerabilities and behavioural biases.

A related concern is the increasing use of "dark patterns" on digital platforms. Dark patterns refer to interface designs that intentionally guide or push users to make decisions that may not be in their best interest.[10] The Guidelines identify thirteen specified categories of dark patterns, including false urgency, basket sneaking, confirm shaming, forced action, subscription trap, interface interference, bait and switch, drip pricing, disguised advertisement, nagging, trick question, SaaS billing, and rogue malwares.

These categories directly cover practices such as misleading subscription options, hidden or unavoidable charges, cumbersome cancellation processes, manipulative consent mechanisms, and deceptive presentation of advertisements. AI systems can further enhance the effectiveness of such practices by adapting interface design, pricing prompts, advertisements, and consent flows on the basis of real-time consumer behaviour. This creates an enforcement challenge because the manipulative design may not be static; it may vary across consumers depending on profiling, behavioural prediction, vulnerability mapping, and personalised experimentation.

Such practices undermine the principle of informed consumer choice, which lies at the heart of the Consumer Protection Act, 2019, the Consumer Protection (E-Commerce) Rules, 2020, and the CCPA Dark Patterns Guidelines, 2023. The E-Commerce Rules are particularly relevant because they impose obligations on e-commerce entities operating digital platforms and seek to prevent unfair trade practices in online consumer transactions. Consumers should be empowered to make decisions based on accurate information, transparent disclosures, and free consent, rather than being subtly manipulated by sophisticated algorithmic systems.

In the context of AI-enhanced personalisation, regulatory scrutiny must therefore examine not only whether a platform's interface is facially misleading, but also whether automated design choices are being used to exploit behavioural

[10] OECD, *Consumer Policy and the Digital Transformation* (2020); Central Consumer Protection Authority, *Guidelines for Prevention and Regulation of Dark Patterns, 2023*, issued under Section 18 of the Consumer Protection Act, 2019.

vulnerabilities or distort consumer autonomy. Thus, there is a growing need for active enforcement of the CCPA Dark Patterns Guidelines, 2023, alongside the Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020, to address deceptive AI-enabled marketing practices and protect consumers from personalised manipulation in digital markets.

E. Liability and Accountability in AI-Driven Systems

One of the most complex legal challenges related to Artificial Intelligence revolves around the issue of liability when AI systems cause harm. Traditional legal frameworks generally assume that decisions are made by identifiable persons or entities who can be held accountable for their actions. However, AI systems often operate autonomously or semi-autonomously, making it difficult to determine responsibility when bad outcomes occur.

For example, an AI-powered medical diagnostic tool may provide inaccurate recommendations, an automated financial system may wrongfully deny credit, or a recommendation algorithm may promote misleading or harmful products. In such situations, determining liability becomes challenging because multiple actors may be involved, including software developers, manufacturers, data providers, platform operators, and service providers.

The complexity of AI systems often creates what researchers refer to as the "accountability gap." Injured consumers may have difficulty identifying the responsible party and obtaining effective remedies. Current consumer protection systems may prove inadequate where harm results from autonomous decision-making processes rather than direct human behaviour.

To address these issues, many researchers and policymakers have advocated for clearer accountability frameworks that distribute responsibility among the stakeholders involved in the development and implementation of AI systems. Such a framework should ensure that consumers have access to effective redress mechanisms and that companies remain accountable for the consequences of AI-driven decisions that affect consumer rights.

F. Existing Legal and Regulatory Frameworks Governing AI and Consumer Protection

The rapid growth of artificial intelligence has prompted governments and regulators around the world to rethink the adequacy of existing legal frameworks. While most jurisdictions do not yet have comprehensive consumer protection legislation specifically targeting AI, a combination of consumer protection laws, data protection regulations, and new AI governance frameworks provides a foundation for addressing the risks associated with AI-powered products and services.

The effectiveness of these legal frameworks depends largely on their ability to adapt traditional consumer protection principles to the realities of automated decision-making, algorithmic processing, and data-intensive business models. The following sections examine the main legal mechanisms currently supporting consumer protection in the era of artificial intelligence.

V. CONSUMER PROTECTION ACT, 2019

In India, the Consumer Protection Act, 2019 represents the primary legislation that safeguards consumer rights against unfair trade practices, misleading advertisements, and defective products and services. Although enacted before the widespread adoption of generative AI technologies, several of its provisions remain relevant to AI-driven markets.[11]

The law recognizes important consumer rights, including the right to information, the right to seek redress, and protection against unfair trade practices. These principles can be applied to situations where AI systems make misleading recommendations, facilitate deceptive advertising practices, or produce results that negatively affect consumers.

However, the law does not specifically address issues such as algorithmic transparency, automated decision-making, or accountability arising from autonomous systems. Thus, while the legislation provides a valuable foundation,

[11] Consumer Protection Act, 2019, No. 35 of 2019 (India)

there is still a need for clear regulatory guidance addressing AI-related consumer injuries.

A. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act), [12] read with the Digital Personal Data Protection Rules, 2025, represents an important step towards strengthening data governance and protecting individual privacy in India's digital ecosystem. Given that Artificial Intelligence systems rely heavily on the collection and processing of personal data, this framework plays an important role in safeguarding consumers from potential misuse of their data.

The DPDP Act is based on principles such as lawful processing of personal data, informed consent, purpose limitation, and data security. The DPDP Rules, 2025 operationalise these principles by prescribing compliance mechanisms relating to notice, consent management, security safeguards, breach notification, and the functioning of the Data Protection Board of India. It provides individuals, as data principals, with rights concerning their personal data, including access to information, correction and erasure of personal data, grievance redressal, and withdrawal of consent.

The Rules further strengthen the consent architecture by recognising consent managers as interoperable platforms through which data principals may give, manage, review, or withdraw consent. These safeguards are particularly relevant in the context of AI-powered products and services, where extensive data collection and profiling often take place without meaningful consumer awareness. The consent-manager framework may assist consumers in exercising greater control over data permissions, although its effectiveness will depend on practical accessibility, platform compliance, and user awareness. The legislation also imposes obligations on data fiduciaries to process personal data responsibly and to implement reasonable security safeguards.

[12] Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.

The DPDP Rules, 2025 additionally provide for a phased compliance timeline, including an eighteen-month transition period for several substantive compliance obligations, thereby allowing organisations time to align technical and operational systems with the statutory framework. Such commitments can help increase consumer trust in AI-enabled services and reduce the risks associated with unauthorized data sharing and data breaches.

Despite these positive developments, certain concerns remain. The DPDP Act and the DPDP Rules primarily address personal data governance and do not comprehensively regulate algorithmic transparency, automated decision-making, explainability, algorithmic bias, or AI-specific consumer liability. Therefore, while the framework strengthens privacy protection and compliance mechanisms, it does not fully address broader consumer protection concerns arising from AI systems.

As a result, although the DPDP framework strengthens privacy protection, consent management, breach response, and institutional enforcement, future reforms may still be necessary to provide stronger safeguards against discriminatory, opaque, or unfair algorithmic practices in consumer-facing AI systems.

B. General Data Protection Regulation (GDPR)

The European Union's General Data Protection Regulation (GDPR) is widely regarded as one of the most comprehensive data protection frameworks in the world. [13]Since many AI systems rely on the processing of personal data, the GDPR provides important safeguards that indirectly promote consumer protection.

A notable feature of the GDPR is its emphasis on transparency and accountability. Organizations are required to inform individuals about how their data is collected, processed and used. The Regulation also recognizes certain protections against decisions based solely on automated processing where such decisions materially affect individuals.

The GDPR promotes principles such as data reduction, fairness, accuracy, and privacy by design. These principles encourage companies to incorporate privacy

[13] Regulation (EU) 2016/679 (General Data Protection Regulation)

considerations throughout the development and deployment of AI systems rather than treating privacy as an afterthought.

The European approach shows how strong data protection laws can support responsible AI governance. Nevertheless, researchers have observed that data privacy alone cannot address all consumer protection concerns related to AI, especially those related to product safety, manipulation, and algorithmic discrimination.

C. The European Union AI Act

Recognizing the limitations of the current legal framework, the European Union has enacted the AI Act, which represents one of the first comprehensive attempts to regulate artificial intelligence directly. [14]The law takes a risk-based approach, classifying AI systems according to the level of risk they pose to individuals and society.

High-risk AI systems, especially those used in sectors such as healthcare, industry, education, and financial services, are subject to strict regulatory requirements. These include obligations relating to transparency, human control, risk management, data quality and accountability.

The AI Act also prohibits certain AI practices that are considered incompatible with fundamental rights and consumer interests. By establishing clear obligations for developers and deployers of AI systems, the legislation seeks to ensure that innovation takes place within an ethically and legally responsible framework.

The European model provides valuable lessons for jurisdictions seeking to regulate AI while protecting consumers. The emphasis on risk assessment, transparency and accountability provides a useful foundation for future AI governance initiatives globally.

VI. COMPARATIVE ANALYSIS OF REGULATORY APPROACHES

The challenges of AI-powered products and services have prompted diverse regulatory responses in different jurisdictions. While there is broad agreement on the

[14] Regulation (EU) 2024/1689 (Artificial Intelligence Act)

need for consumer protection, countries vary considerably in their approaches to regulating artificial intelligence.

A. India

India's approach to AI governance is still evolving. Existing consumer protection and data protection laws provide certain safeguards; however, India has not yet enacted a dedicated binding statute that comprehensively governs AI systems. At the same time, recent policy developments indicate a more structured approach to AI governance. The Ministry of Electronics and Information Technology unveiled the India AI Governance Guidelines on 5 November 2025 under the IndiaAI Mission, setting out a national framework for safe, inclusive, and responsible AI adoption across sectors.

Although the Consumer Protection Act, 2019 and the Digital Personal Data Protection Act, 2023 (DPDP Act) offer partial protection, important issues such as algorithmic accountability, explainability, and AI-specific liability remain largely unaddressed. As AI adoption continues to grow, India may still require clearer enforceable standards for high-risk and consumer-facing AI systems. The current position is therefore best described as a developing governance model: India has not enacted a comprehensive AI statute, but it has moved beyond a purely general-law approach by adopting AI-specific guidelines and sectoral frameworks that seek to balance innovation with consumer welfare, accountability, transparency, and risk management.

B. European Union

The European Union has emerged as a global leader in AI regulation through its proactive and rights-based approach. The combination of the GDPR and the AI Act creates a comprehensive framework that addresses both privacy concerns and AI-specific risks.

The EU model places great emphasis on transparency, accountability, human control and the protection of fundamental rights. By imposing obligations on developers and deployers of high-risk AI systems, the European approach seeks to prevent harm before it occurs, rather than relying solely on remedial mechanisms.

C. United States

The United States has taken a relatively decentralised and increasingly contested approach to AI regulation. Rather than enacting a comprehensive federal AI statute, regulatory oversight has traditionally been carried out through existing institutions, sector-specific regulation, federal executive action, and state-level legislation. However, recent developments have made federal-state regulatory tension a defining feature of the U.S. AI governance landscape.

The Federal Trade Commission (FTC) continues to play an active role in addressing misleading, deceptive, or unfair AI practices, particularly where algorithmic systems cause consumer harm. However, FTC enforcement now operates alongside an unsettled federal pre-emption debate and an expanding body of state AI regulation.[15] While this flexible and institution-based approach may encourage innovation, critics argue that it can result in inconsistent protections for consumers. Conversely, broad federal pre-emption of state AI laws may reduce regulatory fragmentation but may also limit state-level experimentation in areas such as transparency, anti-discrimination, consumer safety, and digital accountability. The U.S. model therefore remains dynamic and unresolved rather than merely sector-specific.

The comparison of these jurisdictions highlights a common challenge: balancing technological innovation with effective consumer protection. While regulatory models vary, there is growing recognition that AI governance must prioritize transparency, accountability, fairness, and consumer welfare.

VII. RECOMMENDATIONS

In light of the challenges identified throughout this study, several measures can be taken to strengthen consumer protection in the era of AI-powered products and services.[16]

1. **Enhancing Algorithmic Transparency:** Users should be provided with important information regarding the operation of AI systems that significantly

[15] Federal Trade Commission, *Aiming for Truth, Fairness and Equity in Your Company's Use of AI* (2021).
[16] NITI Aayog, *Responsible AI for All: Operationalizing Principles for Responsible AI* (2021)

affect their rights and interests. Transparent decision-making processes can improve trust and enable users to challenge unfair outcomes.

2. **Determining Right to Explanation:** Consumers affected by significant automated decisions should have the right to seek explanations regarding the factors that influenced such decisions. This would promote accountability and facilitate the effectiveness of contingency plans.
3. **Strengthen data protection and privacy safeguards:** Organizations should adopt principles of privacy by design and limit data collection to what is necessary for specific purposes. Stronger security measures are needed to prevent excessive control and misuse of user information.
4. **Mandatory AI Audits:** Regular independent audits of high-risk AI systems should be conducted to identify biases, inaccuracies, and discriminatory results. Such audits would help ensure legal and ethical compliance.
5. **Clear Accountability Framework:** Lawmakers should establish clear rules that divide responsibility between developers, manufacturers, service providers, and operators of AI systems. Effective accountability frameworks are essential to ensure consumer access to remedies.
6. **User Awareness and Digital Literacy:** Consumers should be informed about AI technology, data privacy risks and their legal rights. Increased digital literacy can empower consumers to make informed decisions and reduce vulnerability to manipulative practices.

VIII. CONCLUSION

Artificial intelligence has transformed the modern marketplace by enabling unprecedented efficiency, personalization, and innovation. From e-commerce platforms and financial services to healthcare applications and digital assistants, AI-powered products and services have become an integral part of everyday consumer experiences. While these technological advances provide significant benefits, they also pose complex challenges that traditional consumer protection frameworks were not designed to address.

This research has shown that issues such as algorithmic opacity, data privacy issue, discriminatory outcomes, manipulative digital practices, and accountability gap pose significant risks to consumer rights. Although current legal frameworks provide some degree of protection, they often fail to address the specific characteristics of autonomous and data-driven technologies.

The comparative analysis of regulatory approaches reveals an emerging global consensus on the need for greater transparency, accountability, and human oversight in AI governance. While the European Union has made significant strides through the GDPR and AI law, countries like India are still developing their regulatory responses to the rapidly evolving AI landscape.

Ultimately, the future of consumer protection in the era of artificial intelligence depends on the development of adaptive legal frameworks capable of balancing innovation with the protection of fundamental consumer rights. As AI technologies continue to transform economic and social interactions, policymakers, businesses, and regulators must work together to ensure that technological progress remains aligned with the principles of fairness, transparency, accountability, and consumer welfare.[17]

IX. REFERENCES

A. Statutes and Regulations

1. Consumer Protection Act, 2019, No. 35 of 2019 (India).
2. Digital Personal Data Protection Act, 2023 (India); Digital Personal Data Protection Rules, 2025, Ministry of Electronics and Information Technology, Government of India.
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).
4. Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act).

[17] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021)

B. Cases

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
2. Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274.

C. Books

1. Russell, Stuart & Norvig, Peter, *Artificial Intelligence: A Modern Approach* (4th ed., Pearson, 2021).
2. O'Neil, Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown Publishing Group, 2016).
3. Eubanks, Virginia, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* (St. Martin's Press, 2018).
4. Floridi, Luciano, *The Ethics of Artificial Intelligence: Principles, Challenges and Opportunities* (Oxford University Press, 2023).
5. Susskind, Richard, *Tomorrow's Lawyers: An Introduction to Your Future* (3rd ed., Oxford University Press, 2023).

D. Journal Articles

1. Wachter, Sandra, Mittelstadt, Brent & Floridi, Luciano, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," 7(2) International Data Privacy Law 76 (2017).
2. Citron, Danielle K. & Pasquale, Frank, "The Scored Society: Due Process for Automated Predictions," 89 Washington Law Review 1 (2014).
3. Selbst, Andrew D. et al., "Fairness and Abstraction in Sociotechnical Systems," Proceedings of the Conference on Fairness, Accountability and Transparency (2019).
4. Crawford, Kate & Calo, Ryan, "There is a Blind Spot in AI Research," 538 Nature 311 (2016).
5. Martin, Kirsten, "Ethical Implications and Accountability of Algorithms," 160 Journal of Business Ethics 835 (2019).

6. Hildebrandt, Mireille, "The Artificial Intelligence of European Union Law," 21 German Law Journal 74 (2020).
7. Pasquale, Frank, "Restoring Transparency to Automated Authority," 9 Journal on Telecommunications and High Technology Law 235 (2011).

E. Reports and Policy Documents

1. OECD, *Recommendation of the Council on Artificial Intelligence* (2019).
2. OECD, *Artificial Intelligence, Machine Learning and Big Data in Finance* (2021).
3. United Nations Conference on Trade and Development (UNCTAD), *Manual on Consumer Protection* (2020).
4. World Economic Forum, *A Framework for the Responsible Limits on Facial Recognition* (2022).
5. Federal Trade Commission, *Aiming for Truth, Fairness and Equity in Your Company's Use of AI* (2021).
6. UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
7. NITI Aayog, *National Strategy for Artificial Intelligence: #AIforAll* (2018).
8. NITI Aayog, *Responsible AI for All: Operationalizing Principles for Responsible AI* (2021).

F. Online Resources

1. European Commission, "Artificial Intelligence Act", available at https://artificial-intelligence-act.eu
2. OECD AI Policy Observatory, available at https://oecd.ai
3. UNESCO Artificial Intelligence Ethics Portal, available at https://www.unesco.org
4. Ministry of Electronics and Information Technology (MeitY), Government of India, available at https://www.meity.gov.in