

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

A Study on the Role of Artificial Intelligence in E-Commerce and Its Cyber Law Implications

SHANTANU GANGULY* AND SUSHANTA KUMAR DAS**

ABSTRACT

Artificial Intelligence (AI) has emerged as a defining force in the transformation of electronic commerce, enabling businesses to analyze consumer behaviour, personalize recommendations, detect fraud, automate logistics and set dynamic prices with unprecedented speed and scale. While this integration has generated substantial economic efficiency and consumer convenience, it has simultaneously created regulatory and ethical challenges that existing legal frameworks were not originally designed to address. This study examines the role of Artificial Intelligence in e-commerce and analyzes its implications under Indian cyber law, with particular attention to data privacy, algorithmic transparency and bias, cybersecurity, automated decision-making liability, consumer protection and cross-border jurisdiction. Adopting a qualitative, doctrinal-cum-analytical research design, the study draws on statutory provisions, including the Information Technology Act, 2000, the Consumer Protection Act, 2019, the Digital Personal Data Protection Act, 2023 and the Competition Act, 2002, alongside landmark judicial pronouncements such as Justice K.S. Puttaswamy (Retd.) v. Union of India, Shreya Singhal v. Union of India, Anvar P.V. v. P.K. Basheer and Google India Pvt. Ltd. v. Visaka Industries, together with comparative international instruments such as the European Union's Artificial Intelligence Act and the General Data Protection Regulation. These materials are examined through qualitative thematic analysis. The findings indicate that India's cyber law framework provides only partial and fragmented regulation of AI-driven e-commerce, with significant gaps in algorithmic accountability, liability allocation for autonomous decisions and cross-border enforcement. The study concludes that a comprehensive, risk-calibrated legal framework, incorporating algorithmic transparency obligations, strengthened data protection, clear liability rules and ethical governance principles, is essential to reconcile technological innovation with the protection of consumer rights and constitutional privacy guarantees in the digital marketplace.

Keywords: *Artificial Intelligence, E-Commerce, Cyber Law, Data Privacy, Algorithmic Accountability, Consumer Protection, Information Technology Act, Digital Personal Data Protection Act, Intermediary Liability, India*

* Author is a Scholar at ICFAI University, Gangtok, Sikkim, India.

** Author is a Scholar at ICFAI University, Gangtok, Sikkim, India.

I. INTRODUCTION

The rapid evolution of digital technology in the twenty-first century has transformed the global economic landscape, and artificial intelligence has emerged as among the most influential of these innovations. AI refers broadly to the simulation of human intelligence processes by machines and computer systems, enabling them to reason, learn, perceive and make decisions (Russell & Norvig, 2021). Its integration into electronic commerce has changed the way goods and services are produced, marketed, distributed and consumed, allowing digital platforms to extend their operations beyond geographical boundaries and to trade in a genuinely global marketplace.

Major digital corporations such as Amazon, Alibaba Group and Flipkart rely heavily on AI-driven technologies, among them machine learning algorithms, natural language processing, recommendation engines, automated chatbots, predictive analytics and dynamic pricing systems, to analyze consumer data, predict purchasing behaviour, personalize marketing, detect fraud and automate logistics. These capabilities have improved operational efficiency and consumer experience considerably, but they have also generated significant legal and regulatory challenges. Because AI systems depend on the continuous collection, storage and processing of large volumes of personal data, their use raises pressing concerns about privacy protection, cybersecurity, algorithmic transparency and consumer rights.

In India, the regulation of online activity falls primarily within the domain of cyber law, anchored by the Information Technology Act, 2000, which grants legal recognition to electronic records and digital signatures while addressing cybercrime and intermediary liability. That legislation was enacted, however, at a time when artificial intelligence technologies were still nascent, and it does not directly contemplate the autonomous, self-learning and often opaque character of contemporary AI systems. AI-driven systems increasingly take decisions on pricing, transaction approval, content moderation and fraud flagging without direct human intervention, which raises complex questions of liability and accountability when those systems cause harm or infringe consumer rights.

The Indian judiciary has played a formative role in shaping the legal framework applicable to digital technologies. In *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), a nine-judge bench of the Supreme Court recognized the right to privacy as a fundamental right traceable to Article 21 of the Constitution, a ruling with far-reaching implications for AI-driven data processing. In *Shreya Singhal v. Union of India* (2015), the Court struck down Section 66A of the Information Technology Act, 2000 and read down Section 79(3)(b) so that an intermediary

is obliged to disable unlawful content only upon receiving actual knowledge through a court order or an appropriate government notification, emphasizing the need to balance digital regulation with fundamental rights. In *Anvar P.V. v. P.K. Basheer* (2014), the Court clarified the certification requirements governing the admissibility of electronic evidence, a matter of direct relevance to disputes arising from e-commerce transactions, while *Google India Pvt. Ltd. v. Visaka Industries* (2020) confirmed that the statutory immunity available to online intermediaries for third-party content is conditional rather than absolute. Despite these developments, the regulation of artificial intelligence specifically remains an emerging and underdeveloped area of Indian law.

This study therefore examines the role of artificial intelligence in e-commerce and critically analyzes its legal implications within the framework of Indian cyber law. The discussion proceeds by reviewing the existing literature on AI, e-commerce and cyber law; setting out the research gap and objectives; describing the qualitative research methodology; presenting a thematic analysis of the legal issues identified; discussing the findings; and concluding with policy recommendations.

II. REVIEW OF LITERATURE

The literature relevant to this study spans the technological foundations of artificial intelligence, its commercial application in e-commerce, and its regulation under Indian and comparative cyber law. The review that follows synthesizes the principal technical, judicial, statutory and policy sources on which the analysis draws.

Russell and Norvig (2021), in *Artificial Intelligence: A Modern Approach*, define artificial intelligence as the study of intelligent agents that perceive their environment and act so as to maximize their chances of achieving defined goals, supplying the technical vocabulary of machine learning, neural networks and natural language processing on which subsequent legal scholarship depends. Goodfellow, Bengio and Courville (2016), in *Deep Learning*, explain the architecture of the neural networks and deep learning models that underlie modern recommendation engines, fraud-detection systems and natural-language chatbots deployed on e-commerce platforms, and in doing so illustrate the technical opacity that later gives rise to the ‘black box’ problem in legal analysis. Bostrom (2014), in *Superintelligence: Paths, Dangers, Strategies*, examines the long-term risks associated with advanced AI systems and argues for proactive regulatory oversight before such systems acquire capabilities that outpace human control, a caution frequently invoked in policy debates on AI governance. Susskind (2017, 2019), in *Tomorrow's Lawyers* and *Online Courts and the Future of Justice*, examines how

emerging technologies, including AI, are transforming legal institutions and dispute-resolution mechanisms, arguing that regulatory and judicial systems must adapt to technologically mediated commerce and justice delivery.

Duggal (2016), in *Textbook on Cyber Law*, provides a doctrinal account of the Information Technology Act, 2000 and its amendments, emphasizing that Indian cyber law was drafted primarily to facilitate electronic transactions and does not adequately anticipate the autonomous decision-making capacity of AI systems.

Indian judicial authority supplies the constitutional and evidentiary architecture within which AI-driven commerce operates. In *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), the Supreme Court unanimously recognized the right to privacy as a fundamental right under Article 21, establishing constitutional safeguards directly relevant to the personal-data practices of AI-driven e-commerce platforms. In *Shreya Singhal v. Union of India* (2015), the Court struck down Section 66A of the Information Technology Act, 2000 as unconstitutional and clarified that intermediaries are obliged to remove unlawful content only upon a court order or an appropriate government notification, thereby confining the circumstances in which the conditional immunity for algorithmically hosted content is lost. In *Anvar P.V. v. P.K. Basheer* (2014), the Court held that an electronic record adduced as secondary evidence must satisfy the certification requirements then contained in Section 65B of the Indian Evidence Act, 1872; that holding was subsequently doubted and then restored by a three-judge bench in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), which confirmed the mandatory character of the certificate where the original device is not produced. In *Google India Pvt. Ltd. v. Visaka Industries* (2020), the Court examined the liability of online intermediaries for allegedly defamatory third-party content and confirmed that safe-harbour protection is conditional on due diligence and on prompt action once actual knowledge is acquired, a precedent with implications for the responsibility of AI-enabled platforms for algorithmically curated content. Earlier, in *Avnish Bajaj v. State (NCT of Delhi)* (2008), the Delhi High Court considered the criminal liability of an online marketplace operator for an item listed by a third-party user, an early Indian precedent on platform responsibility later relevant to AI-mediated listing and moderation systems.

Comparative European material offers a template against which the Indian position can be measured. The European Union's Artificial Intelligence Act, adopted as Regulation (EU) 2024/1689 and in force since August 2024, establishes a risk-based regulatory model classifying AI systems into minimal, limited, high and unacceptable risk categories, subjecting high-risk applications to mandatory transparency obligations, risk management and conformity

assessment, with the bulk of its obligations applying from August 2026. The Court of Justice of the European Union, in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)* (2014), recognized a qualified ‘right to be forgotten’ in relation to search-engine indexing of personal data, reinforcing the principle that data-processing algorithms remain subject to individual data-protection rights. In *Schrems v. Data Protection Commissioner* (2015) the Court invalidated the Safe Harbour adequacy decision, and in *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems* (2020), commonly called Schrems II, it invalidated the Privacy Shield while upholding standard contractual clauses subject to a case-by-case assessment of the destination jurisdiction, underscoring the complexity that AI-driven, cross-border data flows present. The General Data Protection Regulation itself establishes comprehensive obligations regarding consent, data minimization and automated decision-making, including a qualified right not to be subject to a decision based solely on automated processing, offering a benchmark against which India’s data protection regime may be assessed.

On the Indian policy and statutory side, NITI Aayog (2018), in its National Strategy for Artificial Intelligence, outlines the country’s policy vision for AI development across healthcare, agriculture, education and smart cities, while acknowledging the need for complementary legal safeguards to accompany technological adoption. That vision has since been elaborated by the Ministry of Electronics and Information Technology (2025), whose *India AI Governance Guidelines* adopt a deliberately non-statutory, principles-based approach and state that existing legal frameworks will be adapted rather than displaced by a dedicated AI statute. The Digital Personal Data Protection Act, 2023 establishes India’s first comprehensive data-protection statute, introducing obligations on data fiduciaries and rights for data principals that directly affect AI-driven data processing in e-commerce, and the Digital Personal Data Protection Rules, 2025 have since supplied the operational detail on consent, breach notification and cross-border transfer on a phased commencement schedule. The Consumer Protection Act, 2019, together with the Consumer Protection (E-Commerce) Rules, 2020, imposes transparency obligations on e-commerce platforms concerning seller identity, pricing and grievance redressal, and establishes the Central Consumer Protection Authority to investigate unfair trade practices, including those arising from algorithmic pricing and targeting. The Competition Act, 2002 empowers the Competition Commission of India to investigate digital platforms for abuse of dominant position, predatory pricing and anti-competitive agreements, issues increasingly implicated by AI-driven pricing algorithms and data-driven market power.

Pasquale (2015), in *The Black Box Society*, demonstrates how proprietary algorithms that shape consequential consumer and financial decisions resist scrutiny by regulators and by the individuals they affect, undermining conventional due-process protections in digital commerce. At the international level, the UNCITRAL Model Law on Electronic Commerce (1996), which substantially influenced the drafting of India's Information Technology Act, 2000, established early standards for the legal recognition of electronic records and data messages in cross-border commercial transactions.

A further body of scholarship addresses platform responsibility and algorithmic harm. Decisions such as *Myspace Inc. v. Super Cassettes Industries Ltd.* (2016) and *Kent RO Systems Ltd. v. Amit Kotak* (2017) have clarified that Indian courts require intermediaries to act on specific notice rather than to police their platforms proactively, shaping the liability landscape applicable to AI-enabled marketplaces. Comparative United States jurisprudence contributes from a different direction: *hiQ Labs, Inc. v. LinkedIn Corp.* (2022) addresses the scope of computer-misuse liability for the automated scraping of publicly available profile data, while *Carpenter v. United States* (2018) limits the third-party doctrine by holding that government acquisition of historical cell-site location records is a search for Fourth Amendment purposes. Scholarship on algorithmic bias and discrimination, finally, observes that AI systems trained on historically skewed datasets may reproduce discriminatory outcomes in pricing, recommendation and advertising, prompting calls for mandatory algorithmic transparency and independent auditing mechanisms within e-commerce regulation.

Collectively, this literature demonstrates that while the technical foundations of AI and the doctrinal contours of Indian cyber law are individually well documented, legal scholarship specifically integrating the two, examining how AI's autonomous, data-intensive and opaque character interacts with India's existing statutory and judicial framework governing e-commerce, remains comparatively limited. This study seeks to address that gap.

III. RESEARCH GAP AND OBJECTIVES

Despite growing academic interest in both artificial intelligence and cyber law, there remains a shortage of comprehensive legal research focusing specifically on the intersection of artificial intelligence, e-commerce and cyber law within the Indian context. Existing statutes such as the Information Technology Act, 2000 and the Consumer Protection Act, 2019 regulate discrete aspects of digital commerce but do not directly address the legal issues generated by autonomous, self-learning AI systems, namely algorithmic accountability, automated decision-

making liability and cross-border algorithmic data flows. This study addresses that gap through an integrated doctrinal and qualitative analysis.

The objectives of this study are to examine the concept and technological foundations of artificial intelligence and its application in modern e-commerce; to analyze the legal framework governing digital commerce under Indian cyber law; to evaluate the privacy and data-protection issues associated with AI-driven e-commerce; to examine the role of the judiciary in regulating digital technologies through case law; to identify gaps in the existing legal framework governing AI in e-commerce; and to propose legal reforms and policy recommendations.

The study is guided by four research questions. What is the role of artificial intelligence in modern e-commerce systems? What legal challenges arise from the use of AI in e-commerce platforms? To what extent does the existing cyber law framework regulate AI-driven digital commerce? What legal reforms are necessary to address emerging technological challenges? These questions are examined in light of the primary hypothesis that the increasing integration of artificial intelligence in e-commerce creates significant legal challenges relating to data privacy, cybersecurity and algorithmic accountability, and that the existing cyber law framework in India remains inadequate to regulate these developments effectively.

IV. METHODOLOGY

A. Research design

This study adopts a qualitative, doctrinal-cum-analytical research design. The doctrinal method involves the systematic analysis of legal principles derived from statutes, judicial decisions and academic commentary, while the analytical method is used to evaluate the adequacy of those frameworks in regulating AI-driven e-commerce. A qualitative design is appropriate because the research questions concern the interpretation and adequacy of legal texts and judicial reasoning rather than the measurement of quantifiable variables (Creswell & Poth, 2018).

B. Sources of data

The research relies primarily on secondary sources. These comprise primary legal instruments, including the Information Technology Act, 2000, the Consumer Protection Act, 2019, the Digital Personal Data Protection Act, 2023, the Indian Contract Act, 1872, the law of evidence as contained in the Indian Evidence Act, 1872 and, since 1 July 2024, in the Bharatiya Sakshya Adhiniyam, 2023, and the Competition Act, 2002; judicial decisions of the Supreme Court and High Courts of India, together with comparative decisions of the Court of Justice of the European Union and of United States courts; international regulatory instruments, including the

European Union's Artificial Intelligence Act, the General Data Protection Regulation and the UNCITRAL Model Law on Electronic Commerce; and academic books, journal articles and government policy documents, including NITI Aayog's National Strategy for Artificial Intelligence.

C. Sampling

A purposive sampling strategy was used to select statutes, judgments and scholarly sources. The inclusion criteria required that a source directly address the regulation of AI, e-commerce or digital data processing within a legal or policy context, and that it be traceable to an identifiable legislative, judicial or scholarly authority. This non-probabilistic approach reflects standard practice in qualitative doctrinal legal research, where the aim is analytical depth and conceptual saturation rather than statistical representativeness.

D. Qualitative thematic analysis

The collected material was analyzed thematically, following the six-phase process articulated by Braun and Clarke (2006): familiarization with the material; generation of initial descriptive codes, for example 'algorithmic bias', 'intermediary liability', 'data protection' and 'automated decision-making'; collation of codes into candidate themes; review of the themes against the full data corpus; definition and naming of the final themes; and production of the analytical narrative presented below. Six overarching themes were identified: the commercial role of AI in e-commerce; the statutory framework governing digital commerce; data privacy and protection; algorithmic bias and transparency; cybersecurity risk; and liability, consumer protection and jurisdictional challenges.

E. Limitations

The study is subject to certain limitations. It focuses primarily on the Indian legal framework, drawing on comparative material only for contextual insight. Because artificial intelligence technologies are evolving rapidly, some findings may require periodic revision as new legislation and case law emerge. Case law specifically addressing artificial intelligence remains limited in India, which restricts the extent of direct judicial analysis available, and the study relies on doctrinal legal research rather than on empirical data such as practitioner interviews or platform audits.

V. QUALITATIVE ANALYSIS

A. The commercial role of AI in e-commerce

The analysis confirms that artificial intelligence has become an integral component of modern e-commerce platforms. AI systems enable businesses to generate personalized product recommendations, operate automated customer support through chatbots, implement dynamic pricing strategies, detect fraudulent transactions and optimize logistics and supply-chain management. Global platforms such as Amazon, Flipkart and Alibaba Group use machine learning algorithms to process browsing history, purchase records and location data in order to predict consumer behaviour and tailor marketing strategies. This commercial dependence on continuous data processing is precisely what generates the legal tensions examined in the themes that follow.

B. The statutory framework and its gaps

India's regulation of AI-driven e-commerce is currently distributed across several statutes rather than consolidated in dedicated AI legislation. The Information Technology Act, 2000 grants legal recognition to electronic records and digital signatures and criminalizes offences such as identity theft, data theft and unauthorized access, while Section 79 provides intermediaries with conditional immunity for third-party content, as read down in *Shreya Singhal v. Union of India* (2015) and as confirmed to be conditional rather than absolute in *Google India Pvt. Ltd. v. Visaka Industries* (2020). The conditions on which that immunity depends are elaborated in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which impose due diligence, grievance redressal and takedown obligations. The Consumer Protection Act, 2019 and the Consumer Protection (E-Commerce) Rules, 2020 impose transparency obligations on online platforms and empower the Central Consumer Protection Authority to act against unfair trade practices. The Indian Contract Act, 1872 governs the formation of click-wrap and browse-wrap agreements, while the law of evidence, as interpreted in *Anvar P.V. v. P.K. Basheer* (2014) and reaffirmed in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), imposes strict certification requirements for the admissibility of electronic records; those requirements, formerly contained in Section 65B of the Indian Evidence Act, 1872, now appear in Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, which replaced the 1872 Act with effect from 1 July 2024. The Competition Act, 2002 addresses abuse of dominant position and predatory pricing in digital markets. None of these instruments, however, was drafted with autonomous algorithmic decision-making in contemplation, and consequently none directly addresses algorithmic accountability,

explainability or liability for AI-generated harm, which confirms that India's existing framework provides only partial and fragmented regulation of AI-driven commerce.

C. Data privacy and protection

Privacy emerges as a central concern throughout the analyzed material. AI systems depend on the continuous collection of browsing history, purchase records, location data and financial information, raising the risk of unauthorized surveillance and data misuse. The Supreme Court's recognition of privacy as a fundamental right under Article 21 in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) establishes that individuals must retain control over the dissemination of their personal information, and it imposes constitutional constraints on state action while informing the standards expected of organizations that deploy AI-driven data processing. The subsequent enactment of the Digital Personal Data Protection Act, 2023, and the notification of the Digital Personal Data Protection Rules, 2025, represent a significant statutory response, introducing obligations on data fiduciaries and corresponding rights for data principals. Because the substantive obligations under those Rules commence in phases, however, and because neither the Act nor the Rules contains a right to an explanation of automated decisions comparable to that in the General Data Protection Regulation, the application of the regime to the continuous, adaptive data processing characteristic of machine learning systems remains an evolving area requiring further regulatory clarification.

D. Algorithmic bias and transparency

A recurring concern in the material is the 'black box' character of AI decision-making (Pasquale, 2015). Because AI systems are trained on historical datasets that may embed existing social or economic biases, algorithms used for dynamic pricing, product recommendation or advertising targeting may produce discriminatory outcomes without any deliberate intent on the part of the platform operator. The opacity of these systems complicates the allocation of responsibility when such outcomes occur, since it is often unclear whether liability should rest with the developer of the algorithm, the platform operator or the business deploying the system. Indian law currently imposes no binding transparency or disclosure obligation specific to algorithmic decision-making in commercial contexts. The Ministry of Electronics and Information Technology (2025) has issued governance guidelines that articulate transparency and accountability as guiding principles, but those guidelines are advisory rather than enforceable, and they expressly decline to recommend a dedicated AI statute at this stage. Comparative frameworks such as the European Union's Artificial Intelligence Act, by contrast, attempt to address the same gap through risk-tiered transparency and conformity requirements.

E. Cybersecurity risk

E-commerce platforms store vast quantities of sensitive personal and financial data, which makes them attractive targets for cyberattacks such as hacking, phishing and ransomware. AI systems introduce additional vulnerabilities, including adversarial manipulation, whereby malicious actors deliberately alter input data in order to deceive machine learning models. While the Information Technology Act, 2000 provides offences addressing unauthorized access and data theft, and while *Google India Pvt. Ltd. v. Visaka Industries* (2020) illustrates judicial engagement with platform liability for digital content, the analysis suggests that existing cybersecurity provisions were not designed with AI-specific threat vectors in mind and require targeted regulatory updating.

F. Liability, consumer protection and jurisdiction

Automated decision-making by AI systems, whether approving transactions, denying refunds or setting prices, raises difficult liability questions, because traditional legal doctrine assumes that decisions are made by identifiable human actors. The analysis indicates that Indian law defaults to holding the deploying organization responsible for AI-generated harm rather than treating the AI system as an independent legal actor, an approach consistent with the predominant international position, including that reflected in the European Union's Artificial Intelligence Act, which allocates obligations to providers and deployers. Consumer protection concerns are addressed only partially through the Consumer Protection Act, 2019, which targets unfair trade practices but does not specifically regulate algorithmic manipulation of consumer behaviour, such as the targeting of consumers identified as prone to impulsive purchasing. Finally, because e-commerce transactions routinely cross national boundaries, and because AI systems may process data through distributed, multi-jurisdictional infrastructure, the analysis confirms that jurisdictional fragmentation remains a significant unresolved challenge for Indian regulators. The point is illustrated comparatively by the decisions of the Court of Justice of the European Union in *Schrems v. Data Protection Commissioner* (2015) and *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems* (2020), which struck down successive transatlantic adequacy arrangements and required transfer mechanisms to be assessed against the law of the destination jurisdiction.

VI. DISCUSSION OF FINDINGS

The thematic analysis demonstrates that India's cyber law framework, while substantial in scope, provides only partial regulation of AI-driven e-commerce. Existing statutes address discrete aspects of digital commerce, among them the recognition of electronic records,

consumer transparency, evidentiary standards and competition, but none directly regulates algorithmic accountability or automated decision-making liability, the two issues most distinctive to AI as opposed to earlier forms of digital technology. Judicial decisions, particularly *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) and *Shreya Singhal v. Union of India* (2015), have supplied important constitutional and interpretive safeguards, but those decisions predate the widespread commercial deployment of machine learning and were not formulated with the autonomous and adaptive character of AI in mind.

The analysis also suggests that reform is likely to be most effective where it builds upon, rather than displaces, the existing statutory architecture: strengthening the Digital Personal Data Protection Act, 2023 with AI-specific processing safeguards, supplementing the Consumer Protection Act, 2019 with algorithmic-transparency obligations, and clarifying liability rules within the Information Technology Act, 2000, rather than proceeding through a single freestanding AI statute disconnected from established doctrine. That approach is consistent with the position taken by the Ministry of Electronics and Information Technology (2025), which favours the adaptation of existing frameworks over new primary legislation, and it mirrors the comparative experience of the European Union, where the risk-tiered Artificial Intelligence Act was designed to operate alongside, rather than replace, the General Data Protection Regulation.

VII. CONCLUSION AND RECOMMENDATIONS

This study has examined the role of artificial intelligence in e-commerce and its implications under Indian cyber law through a qualitative, doctrinal-cum-analytical framework. The analysis confirms that AI has become an integral component of digital commerce, that India's existing legal framework provides only partial and fragmented regulation of AI-driven platforms, and that significant gaps remain in the areas of algorithmic transparency, automated-decision liability, cybersecurity and cross-border jurisdiction.

On the basis of these findings, the study makes five recommendations. First, dedicated legal provisions should be enacted to address algorithmic transparency, liability for automated decision-making and regulatory oversight of AI systems used in commerce. Second, data-protection regulation under the Digital Personal Data Protection Act, 2023 and the Rules made under it should continue to be strengthened, with specific rules governing consent, data minimization and automated processing appropriate to machine learning systems. Third, mandatory algorithmic auditing and disclosure mechanisms should be introduced to enable consumers to understand and, where appropriate, to challenge automated commercial decisions. Fourth, cybersecurity infrastructure and threat-specific regulation should be strengthened to

address AI-specific vulnerabilities such as adversarial manipulation. Fifth, greater international regulatory cooperation is needed to address the jurisdictional complexity of cross-border, AI-driven e-commerce.

A balanced regulatory approach, one that protects consumer rights, ensures algorithmic transparency and safeguards constitutional privacy guarantees while continuing to encourage responsible technological innovation, will be essential for the sustainable growth of AI-driven e-commerce in India. Future research may usefully extend this doctrinal analysis through empirical inquiry, including interviews with regulators, platform operators and consumers, and through comparative tracking of risk-tiered frameworks such as the European Union's Artificial Intelligence Act as their obligations come progressively into application.

VIII. REFERENCES

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

Artificial Intelligence Act, Regulation (EU) 2024/1689, 2024 O.J. (L series, 12 July 2024).

Avnish Bajaj v. State (NCT of Delhi), 2008 (150) DLT 769 (Delhi High Court, India).

Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code (2023).

Bostrom, N. (2014). *SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES*. Oxford University Press.

Braun, V., & Clarke, V. (2006). *Using thematic analysis in psychology*. *QUALITATIVE RESEARCH IN PSYCHOLOGY*, 3(2), 77–101.

Carpenter v. United States, 138 S. Ct. 2206 (2018).

Competition Act, No. 12 of 2003, India Code (2002).

Consumer Protection Act, No. 35 of 2019, India Code (2019).

Consumer Protection (E-Commerce) Rules, 2020, Gazette of India, pt. II sec. 3(i) (23 July 2020) (India).

Creswell, J. W., & Poth, C. N. (2018). *QUALITATIVE INQUIRY AND RESEARCH DESIGN: CHOOSING AMONG FIVE APPROACHES* (4th ed.). SAGE Publications.

Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (16 July 2020).

Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

Digital Personal Data Protection Rules, 2025, Gazette of India, pt. II sec. 3(i) (14 November 2025) (India).

Duggal, P. (2016). TEXTBOOK ON CYBER LAW (2nd ed.). LexisNexis.

General Data Protection Regulation, Regulation (EU) 2016/679, 2016 O.J. (L 119) 1.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). DEEP LEARNING. MIT Press.

Google India Pvt. Ltd. v. Visaka Industries, (2020) 4 SCC 162 (India).

Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Case C-131/12, ECLI:EU:C:2014:317 (13 May 2014).

hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180 (9th Cir. 2022).

Indian Contract Act, No. 9 of 1872, India Code (1872).

Indian Evidence Act, No. 1 of 1872, India Code (1872) (repealed with effect from 1 July 2024).

Information Technology Act, No. 21 of 2000, India Code (2000).

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, pt. II sec. 3(i) (25 February 2021) (India).

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

Kent RO Systems Ltd. v. Amit Kotak, 2017 SCC OnLine Del 7201 (India).

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY. (2025). *India AI Governance Guidelines*. Government of India.

Myspace Inc. v. Super Cassettes Industries Ltd., 2016 SCC OnLine Del 6382 (India).

NITI AAYOG. (2018). *National Strategy for Artificial Intelligence*. Government of India.

Pasquale, F. (2015). THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION. Harvard University Press.

Russell, S., & Norvig, P. (2021). ARTIFICIAL INTELLIGENCE: A MODERN APPROACH (4th ed.). Pearson.

Schrems v. Data Protection Commissioner, Case C-362/14, ECLI:EU:C:2015:650 (6 October 2015).

Shreya Singhal v. Union of India, AIR 2015 SC 1523 (India).

Susskind, R. (2017). TOMORROW'S LAWYERS: AN INTRODUCTION TO YOUR FUTURE (2nd ed.). Oxford University Press.

Susskind, R. (2019). *ONLINE COURTS AND THE FUTURE OF JUSTICE*. Oxford University Press.

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW. (1996). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*. United Nations.
