JOURNAL OF ARTIFICIAL INTELLIGENCE AND ROBOTICS
Apr - Jun 2026, VOL. 3, ISSUE 2, pp. 1-9
https://doi.org/10.61577/jaiar.2026.100006

RESEAPRO JOURNALS

ORIGINAL ARTICLE

OPEN ACCESS

Artificial intelligence governance, data privacy and consumer trust: Regulatory challenges for digital commerce in India

Lokanath Patra

Department of Law, Ganjam Law College, Berhampur, Odisha, India

ABSTRACT

AI in digital commerce has transformed companies with personalized marketing, predictive analytics, intelligent customer contact, and automated decision-making. However, worries about customer privacy, algorithmic transparency, data security, and regulatory compliance have made consumer trust essential for sustainable digital business success. Data privacy and compliance in Indian digital commerce are examined to develop consumer trust through AI governance. From 2023 to 2026, the study examines the Digital Personal Data Protection Act, 2023, as well as worldwide AI governance frameworks. This study analyzes statutes, policy documents, court decisions, international regulatory systems, and modern literature using a qualitative doctrinal and comparative research method. The research questions examine (i) how AI-enabled commercial practices affect consumer trust, (ii) whether existing legal architecture addresses privacy and ethical issues in AI-based commerce, and (iii) governance mechanisms to balance technological innovation and regulatory compliance. The study found that conventional artificial intelligence can boost corporate productivity and customer satisfaction, but a lack of transparency, algorithmic bias, excessive data collection, and poor governance erode consumer confidence. Strong AI governance principles, privacy-by-design, ethical AI practices, and effective compliance systems may enhance trust and enable responsible digital innovation. The study concludes with a governance framework for sustainable digital commerce that is grounded in legal compliance, AI ethics, and commercial best practices. The findings should help policymakers, businesses, technology developers, and regulators create trusted AI-enabled commercial ecosystems that balance innovation, consumer rights, and corporate sustainability.

KEYWORDS

Artificial intelligence governance, Digital personal data protection act, Consumer trust, Digital commerce, Data privacy, Regulatory compliance

ARTICLE HISTORY

Received 02 April 2026;
Accepted 23 April 2026;
Published 30 April 2026

Introduction

AI transformed business models, consumer relationships, and governance worldwide. AI has transformed marketplace interactions into intelligent, data-driven ecosystems that analyze consumer preferences, forecast purchasing behavior, personalize marketing, manage supplier chains, and automate customer support. Digital enterprises need AI to improve productivity, enhance customer experience, and remain competitive [1,2].

The internet, smartphones, digital payment infrastructure, and government initiatives like Digital India have driven India's digital economic growth over the past decade. The Digital 2025 India Report shows that 55.3% of the population had internet access in early 2025, while mobile cellular connections exceeded 1.12 billion, demonstrating the country's increasing digital ecosystem [3]. From 2024 to 2025, rapid digitalization will add 49 million internet users. Digital commerce with AI offers potential in retail, banking, insurance, healthcare, logistics, and online markets [4,5].

Online business in India is increasing. AI-enabled customer experiences, rapid commerce, Generation Z involvement, and digital inclusivity will drive digital commerce from US$90 billion to US$250 billion by 2030, according to Google and Deloitte [6]. AI applications, including recommendation engines, conversational chatbots, automated pricing systems, fraud detection algorithms, predictive analytics, and personalized marketing, improve consumer engagement and profitability and are essential for business decision-making.

AI provides benefits but raises concerns about the collection, processing, storage, and commercial use of personal data. AI uses large volumes of consumer data to forecast and automate decisions. Thus, informed consent, algorithmic transparency, profiling, surveillance, discrimination, dark patterns, and cross-border data transfers are key ethical and regulatory challenges. Internet commerce relies on consumer confidence, and such faults damage it. Research shows that accountable, transparent data governance supports online transactions [7,8].

The Digital Personal Data Protection Act, 2023 (DPDP Act), addresses these issues and provides a framework for processing digital personal data in India [9]. The Act balances privacy rights and legitimate corporate interests by establishing Data Fiduciaries, recognizing Data Principal rights, improving consent processes, and promoting responsibility for data processing. The DPDP Rules organized India's privacy policy and established a regulatory framework for the digital economy. While the DPDP Act will improve personal data protection, it does not address AI issues like explainability, automated decision-making, algorithmic fairness, or AI risk governance.

The EU's Artificial Intelligence Act, GDPR, OECD AI Principles, NIST AI Risk Management Framework, and ISO/IEC 42001:2023 demonstrate global consensus that trustworthy AI requires governance mechanisms beyond data protection regulation. Better transparency, accountability, human oversight, fairness, privacy-by-design, and risk-based regulation.

This study reveals that legal compliance alone cannot maintain client confidence in AI-driven digital commerce. Legality, ethics, privacy, cybersecurity, and organizational accountability must guide AI governance. This essay critically

***Correspondence:** Mr Lokanath Patra, Department of Law, Ganjam Law College, Berhampur, Odisha, India. e-mail: lokanath_aisect@rediffmail.com

© 2026 The Author(s). Published by Reseapro Journals. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

investigates the AI governance, data protection, and consumer trust in India's digital commerce ecosystem. From 2023 to 2026, it compares India's legislative structure to the finest global governance models. It recommends a pragmatic governance framework to enable firms to reconcile technology innovation with regulatory compliance and generate consumer trust [Figure 1].



Figure 1. Drivers of sustainable AI-driven digital commerce.

Research Methodology

Qualitative, doctrinal, and comparative research is used to critically assess AI governance, data protection, and customer trust in India's digital commerce environment. It assesses the ability of India's regulatory framework to address AI issues within global governance paradigms.

The Digital Personal Data Protection Act, 2023 (DPDP Act), the Digital Personal Data Protection Rules, and international developments like the EU AI Act and global AI governance standards are covered from January 2023 to June 2026 [9]. This altered AI policy and digital commerce in India and elsewhere.

The study selects authoritative legal, policy, and academic sources on AI governance and digital commerce using purposive documentary sampling. Sample analysis:

- 25 peer-reviewed journal articles on AI governance, consumer trust, and data privacy.
- 10 government papers and policy documents from MeitY, NITI Aayog, RBI, OECD, and European Commission [2,10–13].
- Five internationally acknowledged AI governance frameworks: OECD AI Principles, NIST AI Risk Management Framework , ISO/IEC 42001:2023, GDPR, and EU AI Act [13–15].
- Indian laws such as the Digital Personal Data Protection Act, 2023, Information Technology Act, 2000, and Consumer Protection Act, 2019 [9,16,17].
- Analyzed industry reports from Deloitte, PwC, NASSCOM, IBM, McKinsey, and Google to identify new business practices and market trends [6,18–23].

The following research questions guide the research:

1. How does AI governance impact customer trust in Indian digital commerce?

2. Does the Indian legal system sufficiently control AI-driven digital commerce?

3. What governance framework can organizations use to reconcile technological innovation, regulatory compliance, and consumer trust?

Doctrinal, comparative, and qualitative content analysis were used. A critical review of data privacy and AI-enabled digital commerce legislation, court precedents, and regulations was possible using the doctrinal technique. A comparative review of the Indian regulatory landscape, using global AI governance benchmarks and qualitative content analysis, identified themes of transparency, accountability, privacy protection, algorithmic fairness, cybersecurity, and consumer trust.

This study proposes an integrated AI governance framework that encompasses legal compliance, ethical AI principles, privacy-by-design, cybersecurity, and organizational duties. The paper advises politicians, regulators, enterprises, and digital commerce platforms on how to develop trust in AI systems that promote sustainable innovation and customer confidence (Table 1).

Table 1. Research design at a glance.

Component	Description
Research design	Qualitative, doctrinal and comparative study
Study period	January 2023 – June 2026
Research approach	Analytical and exploratory
Sampling technique	Purposive documentary sampling
Sample	25 journal articles, 10 policy reports, 5 international AI frameworks, relevant statutes and industry reports
Data sources	Primary and secondary sources
Methods of analysis	Doctrinal analysis, comparative legal analysis and qualitative content analysis
Research output	Proposed AI governance framework for digital commerce

AI Governance and Consumer Trust in Digital Commerce

AI has transformed digital commerce by automating decision-making, personalizing customer experiences, simplifying

© 2026 Reseapro Journals
https://doi.org/10.61577/jaiar.2026.100006

supply chains, detecting fraud, and enhancing operational efficiency. E-commerce platforms need AI-powered machine learning, NLP, predictive analytics, computer vision, and generative AI. These technologies use enormous amounts of structured and unstructured consumer data to predict buying behavior, recommend products, optimize marketing, establish prices, and engage consumers [1].

India's digital commerce ecosystem benefits from AI. AI-driven recommendation systems, intelligent chatbots, fraud-detection algorithms, inventory optimization tools, and personalized marketing campaigns help Amazon India, Flipkart, Myntra, Reliance JioMart, Tata Neu, and other fintech companies improve customer satisfaction and operational performance. India has one of the quickest AI adoption rates. NASSCOM predicts productivity, automation, and digital innovation will add $500 billion by 2025 [20]. AI might increase company competitiveness and add US$15.7 trillion to the global economy by 2030, according to PwC [19].

AI customizes customer experiences, adding significant financial value. The algorithms use your browsing history, shopping history, demographics, and behavior to recommend products. Companies use predictive analytics to forecast demand, reduce inventory costs, and improve supply chain efficiency. AI chatbots save costs and provide real-time service. To optimize profits, dynamic pricing algorithms alter product prices based on demand, competition, customer behavior, and market conditions.

AI-driven digital commerce collects and processes personal data rather than supporting the economy. Every online transaction leaves personal data, browsing history, purchase decisions, payment information, location data, and behavioral patterns [24]. The datasets improve client profiles and help corporations forecast future purchases. However, excessive use of personal data raises concerns about privacy, informed consent, surveillance, algorithmic discrimination, and abuse [8].

Consumer trust is essential for sustainable digital commerce. According to Mayer, Davis, and Schoorman, trust is the willingness to be vulnerable based on expertise, integrity, and care [7]. Digital customers increasingly want firms to collect exactly the data they need, handle it transparently, protect it against attacks, and give them meaningful control over their personal data. Failure to achieve these expectations can damage brand image, consumer confidence, and regulatory scrutiny, reducing customer retention.

Artificial intelligence governance involves creating principles, norms, institutional procedures, and accountability systems to ensure ethical AI conduct throughout its life cycle. In addition to legal compliance, AI governance encompasses ethical principles such as openness, fairness, explainability, responsibility, privacy, human monitoring, and cybersecurity. Human-centric AI governance that promotes innovation and preserves fundamental rights is being promoted by the OECD, UNESCO, and EU [2,25–27].

Good AI governance requires transparency. Consumers must understand how AI affects credit, product recommendations, price, and buying. Explainable AI can boost customer confidence and reduce information asymmetry by explaining algorithmic decisions. Algorithmic accountability encourages firms to evaluate AI models and hold automated systems accountable to prevent bias and discrimination.

Trustworthy AI needs privacy protection, too. Artificial intelligence must protect privacy in accordance with Cavoukian's 2011 Privacy by Design proposal [28]. Minimization, purpose limitation, informed consent, and safe data handling improve privacy and regulatory compliance. These methods allow firms to safely use AI without violating consumer rights.

Cybersecurity builds customer trust. Traditional AI systems manage massive volumes of sensitive personal data, making them vulnerable to hackers. Access management, encryption, continuous surveillance, AI model validation, and periodic security audits reduce corporate risk and safeguard data confidentiality, integrity, and availability.

The organization's strategic asset is consumer trust, not a behavioral outcome. AI governance and ethical business practices will boost consumer loyalty, regulatory compliance, corporate reputation, and long-term competitiveness. Bad governance can lead to legal liability, reputational harm, financial losses, and consumer distrust. Sustainable digital commerce requires technological innovation and responsible AI governance, with transparency, accountability, privacy, and cybersecurity (Table 2).

Table 2. Business benefits of AI and associated governance challenges.

AI Applications in digital commerce	Business benefits	Governance challenges
Recommendation systems	Personalized shopping experience	Consumer profiling and privacy concerns
Predictive analytics	Improved demand forecasting	Algorithmic bias and data quality
Dynamic pricing	Revenue optimization	Price discrimination and fairness
AI chatbots	Enhanced customer support	Transparency regarding automated interactions
Fraud detection	Financial security	False positives and accountability
Targeted advertising	Higher conversion rates	Behavioral tracking and informed consent
Generative AI	Marketing efficiency and content creation	Intellectual property, misinformation, and accountability

Source: Developed by the author based on Russell & Norvig; OECD; NIST; Cavoukian [1,2,14,28].

Regulatory Challenges and Comparative Perspective

AI has outpaced legal and regulatory institutions, creating governance challenges for governments, organizations, and consumers worldwide. AI has improved digital commerce efficiency, personalization, and economic innovation, but it has also raised legal, ethical, and technological concerns about privacy, transparency, accountability, discrimination, and cybersecurity [8]. These concerns have prompted governments worldwide to balance innovation and individual rights in regulatory regimes.

The DPDP Act, 2023, governs the Indian digital economy. Act's Data Principal and Data Fiduciary rights and duties form a rights-based model of digital personal data processing. Lawful processing, consent-based data acquisition, purpose limitation, data accuracy, security, and grievance redressal are required. It establishes the Data Protection Board of India to enforce compliance and address violations. These guidelines strengthen

© 2026 Reseapro Journals
https://doi.org/10.61577/jaiar.2026.100006

India's digital privacy law and set it as an international standard [9].

The DPDP Act covers personal data processing but not AI. The law does not cover algorithmic explainability, automated decision-making, AI risk classification, discrimination, human monitoring, AI model auditing, or autonomous system accountability. AI corporations can comply with data protection rules while using opaque or biased algorithms that hurt customers. AI technologies are transforming credit approvals, employment recruiting, insurance underwriting, digital marketing, tailored pricing, and customer profiling, deepening this regulatory gap.

The Information Technology Act, 2000, and Consumer Protection Act, 2019, control cybercrime, unfair trade practices, and deceptive advertising [16,17]. Both policies predate generative AI and do not address autonomous decision-making, deepfakes, AI-generated misinformation, or algorithmic accountability. India has no AI law, but the RBI and SEBI have established cybersecurity and digital governance guidelines.

The EU AI Act classifies artificial intelligence systems by their potential impact on health, safety, and fundamental rights. Regulations classify AI uses as unacceptable, high, limited, or moderate risk. Before being sold, high-risk AI systems must meet standards for transparency, human supervision, data quality, risk management, technical documentation, and conformity assessment [26]. This proactive regulatory architecture will safeguard personal data and trust in conventional AI systems throughout their lifespans.

The EU's GDPR is one of the most comprehensive data privacy laws. The GDPR includes data minimization, accountability, storage limits, privacy by design, and openness in addition to privacy as a right. While AI in decision-making is problematic, Article 22 shields humans from automated processing-based choices that have substantial legal or other implications [29].

Many international organizations have AI governance principles and guidelines. The OECD AI Principles promote inclusive growth, transparency, robustness, accountability, and human-centered AI. The NIST AI Risk Management Framework (AI RMF 1.0) helps firms discover, assess, mitigate, and monitor AI risks throughout the system's lifespan [14]. The first global AI governance standard, ISO/IEC 42001:2023, formalizes responsible AI governance through continuous improvement, risk management, documentation, and corporate accountability [15].

India's AI-led digital commerce is successful globally, but regulatory challenges persist. Artificial intelligence systems based on poor data can discriminate in pricing, creditworthiness, employment, and digital services due to algorithmic bias. Customers distrust automated decisions since they do not understand them. Dark patterns and personalized ads influence customers. Cloud infrastructure across borders poses jurisdictional, regulatory, and data transmission challenges.

Cybersecurity is important too. AI systems are vulnerable to hackers, ransomware, data leaks, and model poisoning since they continually access enormous datasets. Generative AI might lead to synthetic identity fraud, phishing, deepfake tools, and AI-powered disinformation campaigns that undermine confidence in digital commerce.

Indian law is necessary yet insufficient for AI governance. While the DPDP Act safeguards personal data, sustainable AI governance requires laws on privacy, algorithmic accountability, explainability, human oversight, cybersecurity, risk management, and ethical AI. Corporate governance integration will boost ethical growth, customer trust, and growth in the digital economy (Table 3).

Table 3. Comparative analysis of AI governance frameworks.

Regulatory framework	Data privacy	AI governance	Explainability	Human versight	Risk-based regulation	Algorithmic accountability
DPDP Act, 2023 (India) [9]	✓	Limited	✕	✕	✕	Limited
Information Technology Act, 2000 [16]	Partial	✕	✕	✕	✕	✕
Consumer Protection Act, 2019 [17]	Partial	Limited	✕	✕	✕	Partial
GDPR (European Union) [29]	✓✓✓	Partial	✓	✓	Partial	✓✓
EU AI Act [26]	✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓	✓✓✓
OECD AI Principles [2]	✓	✓✓	✓✓	✓✓	✓	✓✓
NIST AI RMF 1.0 [14]	Partial	✓✓✓	✓✓	✓✓	✓✓✓	✓✓✓
ISO/IEC 42001:2023 [15]	✓	✓✓✓	✓✓	✓✓	✓✓	✓✓✓

Legend: ✓✓✓ = Comprehensive; ✓✓ = Strong; ✓ = Moderate; Partial = Indirect Coverage; ✕ = Not Specifically Addressed.

Source: Compiled by the Author based on the DPDP Act, 2023; GDPR; EU AI Act; OECD AI Principles; NIST AI RMF 1.0; ISO/IEC 42001:2023 [9,13–15,26,29].

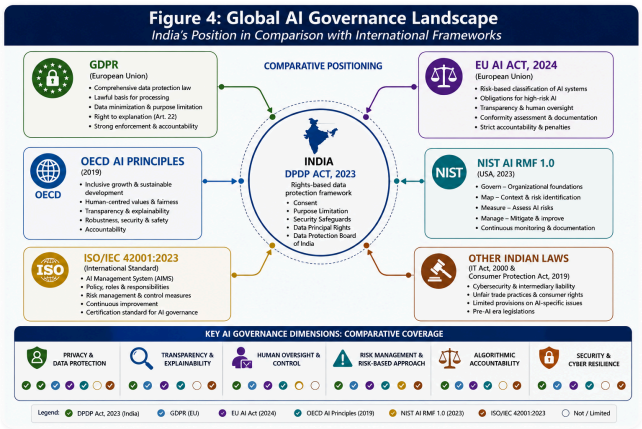

Figure 2. Global AI governance landscape.

Findings and the TRUST-AI Governance Framework for Digital Commerce

This study finds that AI has enhanced digital commerce's efficiency, scalability, and competitiveness, but not regulation. AI-based business models collect, process, and analyze

© 2026 Reseapro Journals
https://doi.org/10.61577/jaiar.2026.100006

consumer data for personalization, automated decision-making, predictive analytics, dynamic pricing, fraud detection, and intelligent customer contact. These technologies are economically promising but have governance issues that diminish client confidence [30].

The DPDP Act, the Information Technology Act, 2000, the Consumer Protection Act, 2019, the GDPR, the EU AI Act, the OECD AI Principles, the NIST AI Risk Management Framework, and ISO/IEC 42001 provide key findings [13–17,26].

Major findings

Finding 1: AI growth in digital commerce is exponential, whereas legal and regulatory systems evolve slowly. Technological innovation exceeds regulatory readiness.

Finding 2: The DPDP Act, 2023, protects personal data but does not address AI governance issues, including algorithmic transparency, explainability, autonomous decision-making, AI model audits, and human oversight.

Finding 3: Legal compliance, organizational openness, ethical AI techniques, effective cybersecurity, and responsible data management progressively influence consumer trust.

Finding 4: International regulatory frameworks require enterprises to identify, monitor, and mitigate AI-related risks throughout the system lifecycle.

Finding 5: Most companies view AI governance as a compliance need rather than a strategic business management tool.

Finding 6: Responsible AI governance boosts consumer loyalty, company reputation, regulatory compliance, operational resilience, and competitive advantage, sustaining businesses.

Proposed TRUST-AI governance

This study offers the TRUST-AI Governance Framework for AI-driven digital commerce based on these findings. Consumer trust underpins digital commerce, but unified legal, technological, ethical, and organizational management is needed. In the suggested concept, TRUST represents five interconnected governance pillars.

T — Transparency

Businesses must disclose the use of AI in client interactions and automated decision-making. Customers should know when AI affects product suggestions, tailored marketing, price, or service. Explainable AI should explain crucial automated decisions. Disclosure raises business-consumer awareness and accountability.

R — Responsibility

Companies must be held liable for the use of AI. Inform top management, AI ethics, regulatory compliance, risk assessment, and monitoring committees.

Humans should be involved in high-impact decisions to prevent automated technology from replacing human judgment in sensitive commercial situations.

U — User Privacy

AI Lifecycle Privacy by Design should transcend regulations. Organizations should utilize informed consent, data minimization, purpose limitation, secure data retention, and customer rights management. Businesses must grow responsibly and give consumers control over their data.

S — Security

Trustworthy AI governance requires cybersecurity. AI cybersecurity protects AI models and customer data with encryption, authentication, vulnerability assessments, adversarial testing, incident response planning, and security audits.

T—Trust building

AI governance seeks consumer trust. Transparent grievance redress, AI audits, ethical AI policies, and stakeholder communication are essential. Trust boosts consumer loyalty, regulatory confidence, and corporate longevity.

Practical implementation framework

Multiple departments must collaborate for the TRUST-AI Framework to succeed.

- The Board of Directors should incorporate AI governance into corporate governance and risk management.
- Compliance Officers oversee sectoral and worldwide AI governance standards under the DPDP Act.
- Technology Teams must develop AI systems that prioritize explainability, justice, privacy, and cybersecurity [31].
- Business managers should balance commercial innovation with ethical decision-making and establish customer trust using AI.
- Provide consumers with clear information about automated processing, grievance resolution, and data control.

Business significance of the framework

The TRUST-AI Governance Framework does not require AI governance compliance, unlike previous techniques. The framework helps organizations establish consumer trust, minimize regulatory and legal risk, improve accountability, brand image, responsible innovation, international compliance, customer loyalty, and sustainable digital commerce. Digital commerce companies that use trusted AI tools can integrate technical governance, legal compliance, and commercial strategy (Table 4 and Figure 3).

Source: Developed by the author.

Table 4. Components of the proposed TRUST-AI governance framework.

Pillar	Core objective	Key implementation measures	Expected business outcome
Transparency	Explainable AI and disclosure	AI notices, explainability reports, and algorithm disclosure	Consumer confidence
Responsibility	Organizational accountability	AI governance committee, human oversight, audits	Regulatory compliance
User privacy	Protection of personal data	Privacy by design, consent management, data minimization	Privacy protection
Security	Protection of AI systems and data	Encryption, cybersecurity audits, and incident response	Operational resilience
Trust building	Long-term consumer confidence	Grievance mechanisms, ethical AI policies, stakeholder engagement	Customer loyalty and sustainable growth

© 2026 Reseapro Journals
https://doi.org/10.61577/jaiar.2026.100006

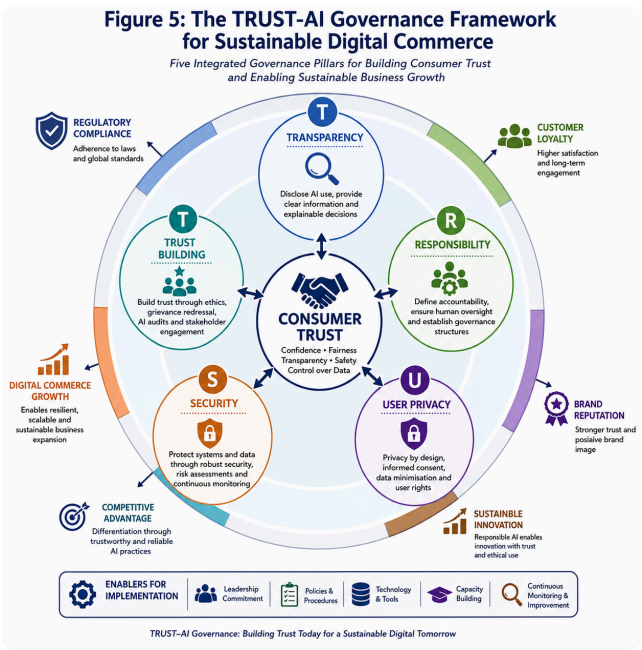

Figure 3. The TRUST-AI governance framework for sustainable digital commerce.

Policy Implications and Recommendations

This study found that while Artificial Intelligence (AI) has encouraged innovation and competition in digital commerce, its sustainable deployment requires solid governance mechanisms that protect consumer rights and promote technological growth. Innovation, regulatory compliance, ethical AI, and customer trust compose the TRUST-AI Governance Framework. Policymakers, regulators, corporations, technology developers, and consumers must cooperate for implementation (Table 5 and Figure 4) [7] .

Policy implications

This report affects Indian policy. AI-specific regulation is fragmented, but the 2023 Digital Personal Data Protection Act provides a solid framework [10]. Thus, beyond data privacy legislation, governments should build a national AI governance framework with algorithmic accountability, explainability, human oversight, fairness, and AI risk management. A risk-based regulatory framework, such as the EU Artificial Intelligence Act, would enable regulators to classify AI systems by impact and assign compliance duties. Innovation and consumer protection would result from this strategy. The government may create an AI Regulatory Authority or AI Governance Division to coordinate AI standards, certification, compliance monitoring, and inter-agency cooperation in the digital governance ecosystem. The Data Protection Board of India might control AI with this institutional framework.

Implications for businesses

Digital commerce businesses should consider AI governance a business strategy rather than a legal mandate [6,18]. Ethical AI corporate governance may boost consumer confidence, brand reputation, and competitiveness, and reduce the risk of lawsuits. Businesses need AI Ethics or Governance Committees to develop policy, assess risk, audit algorithms, and comply with regulations. AI should follow Privacy-by-Design and Security-by-Design during system design, deployment, monitoring, and evaluation [28]. Before implementing high-risk AI applications that affect pricing, credit, consumer profiles, employment, healthcare, or financial services, AI Impact Assessments should be routine. Regular independent AI audits should assess fairness, transparency, robustness, and cybersecurity.

Implications for regulators

Government, industry, academia, and civil society should work on regulatory governance. The e-commerce, fintech, healthcare, insurance, logistics, education, and digital marketing sectors may collaborate on AI governance rules. Regulators should promote ISO/IEC 42001:2023, NIST AI Risk Management Framework, and OECD AI Principles [15]. Global governance would promote India's digital commerce and competitiveness [21]. Expanding regulatory sandboxes to test breakthrough AI technology under regulatory control fosters responsible innovation without compromising consumer safety.

Implications for technology developers

AI engineers must provide ethical, transparent, explainable, and safe intelligent systems throughout their lifespans. Technical teams building AI should use explainable AI, bias detection, privacy-enhancing technology, and continuous monitoring. Developers should record datasets, model design, validation, risks, and decisions. Documentation boosts organizational responsibility, regulatory compliance, independent audits, and consumer confidence.

Implications for consumers

Digital commerce relies on consumer trust. Information about AI-enabled digital platform decision-making should be transparent and available to customers. Businesses should offer meaningful consent, privacy notices, grievance redress, and human review of major automated decisions. To help clients grasp the pros and cons of AI-enabled digital services, governments, schools, and industry groups can encourage AI literacy and digital awareness [32].

Recommendations

The following are the Study-based recommendations:

1. Develop a comprehensive AI Governance Framework to support the Digital Personal Data Protection Act, 2023

2. Implement a risk-based regulation paradigm for AI systems considering their societal impact

3. Require AI Impact Assessments for high-risk digital commerce applications

4. Establish AI Governance Committees for large-scale AI deployments

5. Enhance Privacy-by-Design and Security-by-Design in AI lifecycle

6. Encourage Explainable AI to boost customer trust and transparency

7. Conduct regular independent AI audits to assess fairness, accountability, and cybersecurity

8. Promote international standards like ISO/IEC 42001, NIST AI RMF, and OECD AI principles

9. Improve AI literacy initiatives for consumers, corporations, and government officials

© 2026 Reseapro Journals
https://doi.org/10.61577/jaiar.2026.100006

10. Foster global collaboration for AI governance and digital commerce

Table 5. Stakeholder-wise policy recommendations.

Stakeholder	Key recommendations	Expected outcome
Government	Develop dedicated AI governance legislation; establish AI regulatory mechanisms.	Stronger regulatory certainty and responsible innovation
Regulators	Adopt risk-based AI regulation; issue sector-specific guidelines; encourage regulatory sandboxes.	Effective oversight and harmonized compliance
Businesses	Establish AI Governance Committees; conduct AI impact assessments; implement periodic audits.	Increased consumer trust, compliance, and competitiveness
Technology developers	Integrate Explainable AI, Privacy-by-Design, fairness testing, and cybersecurity controls.	Ethical, transparent, and trustworthy AI systems
Consumers	Improve AI literacy; strengthen grievance redressal and consent mechanisms	Greater consumer empowerment and confidence
Academic institutions	Promote interdisciplinary research and AI governance education	Capacity building and evidence-based policymaking

Source: Developed by the author.



Figure 4. Stakeholder ecosystem for responsible AI governance in digital commerce.

Conclusion and Future Research Directions

AI has changed how digital economy organizations communicate with customers, function, and make money. Intelligent automation, predictive analytics, targeted marketing, fraud detection, and data-driven decision making boost efficiency in AI-powered digital commerce. AI adoption poses legal, ethical, and governance challenges about data privacy, algorithmic transparency, accountability, cybersecurity, and consumer protection. These issues must be solved for technology innovation to boost economic growth and customer confidence.

In 2023-2026, this analysis examined AI governance, data protection, and customer trust in India's digital commerce environment. Using a qualitative doctrinal and comparative analysis of the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, the Consumer Protection Act, 2019, and internationally recognized frameworks like the GDPR, the EU Artificial Intelligence Act, the OECD AI Principles, the NIST AI Risk Management Framework, and ISO/IEC 42001.

The DPDP Act in India is a data security milestone, but it prioritizes personal data over AI management. Discussed are algorithmic explainability, AI risk classification, automated decision-making, human oversight, accountability, and AI auditing. Governance for AI-using organizations should include ethical, technological, organizational, and strategic dimensions as well as legal compliance.

The survey also revealed that client trust underlies digital trading. Organizational transparency, responsibility, privacy, cybersecurity, justice, and responsible innovation establish trust beyond legal compliance. Customers want clear, safe, non-discriminatory, and rights-respecting AI technologies. Meeting expectations boosts brand visibility, consumer loyalty, regulatory compliance, and long-term competitiveness.

This paper's main contribution is the TRUST-AI Governance Framework, an integrated governance architecture comprising Transparency, Responsibility, User Privacy, Security, and Trust Building. The paradigm views AI governance as a strategic management function that includes legal compliance, corporate governance, ethical AI, cybersecurity, and consumer-centric business practices. The framework helps policymakers, regulators, corporations, and technology developers build dependable AI systems for sustainable digital commerce.

The report suggested risk-based legislation, mandated AI effect assessments, explainable AI, human oversight, periodic algorithmic audits, and conformity with international norms for Indian AI governance. AI governance must be integrated into organizations through governance committees, Privacy-by-Design, Security-by-Design, constant surveillance, and transparent stakeholder involvement. Constraints would improve consumer confidence, ethical innovation, and global competitiveness.

Limitations of the Study

It ignores consumer viewpoints and organizational AI governance in favor of doctrinal and comparative study. Governance models may need to change quickly as AI regulation evolves. Limits enable scholarly research.

Consumers, corporations, and regulators can study AI governance. Comparative study on AI governance across

© 2026 Reseapro Journals
https://doi.org/10.61577/jaiar.2026.100006

jurisdictions, sector-specific analyses of AI deployment in fintech, healthcare, insurance, education, and e-commerce, and quantitative assessments of AI governance maturity and consumer trust will increase understanding. A longitudinal research may explore how regulations affect business innovation, digital competitiveness, and customer behavior.

Finally, AI governance should support sustainable digital commerce rather than be a legal or technological need. Governments, regulators, corporations, technology developers, and consumers must collaborate to advance innovation in the digital economy and defend fundamental rights. Responsible AI, data protection, and consumer-centric governance can boost trust and create an inclusive, safe, and resilient digital economy (Table 6).

Table 6. Key contributions of the present study.

Contribution	Description
Theoretical contribution	Integrates AI governance, data privacy, and consumer trust into a unified conceptual framework for digital commerce.
Methodological contribution	Employs doctrinal, comparative legal, and qualitative content analysis using Indian and international regulatory frameworks (2023–2026).
Policy contribution	Identifies regulatory gaps in India's AI governance landscape and recommends a risk-based governance approach.
Practical contribution	Develops the original TRUST-AI Governance Framework for adoption by businesses, regulators, and policymakers.
Business contribution	Demonstrates how responsible AI governance enhances consumer trust, regulatory compliance, brand reputation, and sustainable business growth.

Acknowledgements

The author gratefully acknowledges the academic support and research environment provided by the Department of Law at Berhampur University and Ganjam Law College, Berhampur, which facilitated the completion of this research.

Conflict of Interest

The author declares that there are no conflicts of interest related to this manuscript.

Funding

This research received no external funding.

Data Availability Statement

No primary datasets were generated or analyzed during this study. The research is based exclusively on publicly available statutes, judicial decisions, government reports, policy documents, international regulatory frameworks, and scholarly literature cited in the manuscript.

Ethics Statement

This research is based exclusively on doctrinal legal research and documentary analysis using publicly available sources. No human participants, personal data, surveys, interviews, or animal subjects were involved. Therefore, ethical approval and informed consent were not required.

AI Disclosure Statement

Artificial Intelligence-assisted tools were used solely for language refinement, grammar checking, formatting assistance, and improving readability during manuscript preparation. The conceptualization, legal analysis, comparative evaluation, development of the TRUST-AI Governance Framework, interpretation of legal materials, and all scholarly conclusions were independently conceived, verified, and approved by the author. The author accepts full responsibility for the originality, accuracy, and integrity of the manuscript.

References

1. Russell S, Norvig P. Artificial intelligence: A modern approach (4th ed.). 2021.
2. OECD. AI Principles. 2024.
3. DataReportal. Digital 2025: India. 2025.
4. Reserve Bank of India. Report on Trend and Progress of Banking in India. 2024.
5. Reserve Bank of India. Annual report 2024–25. 2025.
6. Google & Deloitte. Digital commerce in India: Trends and future opportunities. 2025.
7. Mayer RC, Davis JH, Schoorman FD. An Integrative Model of Organizational Trust. The Academy of Management Review. 1995;20(3):709. https://doi.org/10.5465/amr.1995.9508080335
8. Acquisti A, Taylor C, Wagman L. The economics of privacy. J Econ Lit. 2016;54(2):442–492. https://doi.org/10.1257/jel.54.2.442
9. Government of India. Digital Personal Data Protection Act. Ministry of Law and Justice. 2023.
10. Ministry of Electronics and Information Technology. Digital Personal Data Protection Act, 2023. 2023.
11. NITI Aayog. Responsible AI for All: Approach document—Part 1: Principles for responsible AI. Government of India. 2021.
12. NITI Aayog. Responsible AI for All: Approach document—Part 2: Operationalizing principles for responsible AI. Government of India. 2021.
13. OECD. OECD Principles on Artificial Intelligence. 2019.
14. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). 2023. https://doi.org/10.6028/nist.ai.100-1.
15. International Organization for Standardization. ISO/IEC 42001:2023—Information technology—Artificial intelligence—Management system. 2023.
16. Government of India. Information Technology Act, 2000 (Act No. 21 of 2000). Ministry of Electronics and Information Technology. 2000.
17. Government of India. Consumer Protection Act, 2019 (Act No. 35 of 2019). Ministry of Consumer Affairs, Food and Public Distribution. 2019.
18. Deloitte. AI and the future of digital commerce. Deloitte Insights.
19. PwC. Sizing the prize: What's the real value of AI for your business?. 2024.
20. NASSCOM. AI adoption in India: Opportunities and challenges. 2024.
21. IBM. Global AI Adoption Index 2024. 2024.
22. McKinsey & Company. The State of AI in 2023. 2023.
23. Google Spain SL v. Google Spain SL v. 2014.
24. National Payments Corporation of India. National Payments Corporation of India. (2025). 2025.
25. UNESCO. Recommendation on the ethics of artificial intelligence. 2021.

© 2026 Reseapro Journals

https://doi.org/10.61577/jaiar.2026.100006

26. European Parliament and Council. Regulation (EU) 2024/1689 laying down harmonized rules on Artificial Intelligence (the Artificial Intelligence Act). Official Journal of the European Union. 2024.
27. Shneiderman B. Human-centered AI. 2022.
28. Cavoukian A. Privacy by Design: The 7 foundational principles. Information and Privacy Commissioner of Ontario. 2011.
29. European Parliament and Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union. 2016:1–88
30. World Economic Forum. Global risks report 2024. 2024.
31. Justice KS. Puttaswamy (Retd.) v. 2017.
32. Internet and Mobile Association of India. Digital in India Report. 2024.

© 2026 Reseapro Journals

https://doi.org/10.61577/jaiar.2026.100006