IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

Technology, AI and Digital Governance, Electronic Evidences and BSA 2023

Charusheela Jaiswar
Vasantdada Patil Pratishthan's Law College, Sion, Mumbai.
E-mail: charu_jaiswar@yahoo.com

Abstract: ***Background:*** *The rapid integration of Technology and Artificial Intelligence (AI) into governance has transformed public administration, regulatory enforcement, and judicial processes worldwide. Global policy frameworks developed by institutions such as the United Nations, OECD, and the European Union emphasize transparency, accountability, human rights, and ethical AI deployment. In India, digital governance reforms have been reinforced by statutory modernization, notably through the enactment of the Bhartiya Saksha Adhiniyam, 2023, which updates evidentiary principles to address electronic and AI-generated evidence.*

Methods:

This paper adopts a doctrinal and comparative research methodology. It analyses international AI governance principles and examines their influence on India's constitutional and statutory framework. The study undertakes a critical review of legislative provisions relating to electronic records, digital signatures, forensic technologies, and admissibility standards under the Bhartiya Saksha Adhiniyam, 2023, supported by relevant judicial interpretations and policy documents.

Results:

The analysis reveals that India's legal reforms demonstrate significant alignment with emerging global norms on digital accountability and evidentiary reliability. The Bhartiya Saksha Adhiniyam, 2023 strengthens recognition of electronic evidence and facilitates digital adjudication. However, concerns persist regarding algorithmic bias, authentication of AI-generated content, data integrity, cybersecurity risks, and the scope of judicial scrutiny over automated decision-making systems.

Conclusions:

The study concludes that effective digital governance requires a balanced regulatory approach that integrates technological innovation with constitutional safeguards. While India's legislative reforms represent a progressive step toward modernizing legal processes, sustained oversight mechanisms,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

ethical AI standards, and institutional capacity-building are essential to ensure transparency, fairness, and protection of fundamental rights in an increasingly AI-driven governance ecosystem.

Keywords: Artificial Intelligence; Digital Governance; Electronic Evidence; Bhartiya Saksha Adhiniyam 2023.

I. INTRODUCTION

Rapid developments in artificial intelligence (AI), quantum computing, and other emerging technologies are transforming the global technological landscape. These changes require governments and institutions to reassess existing governance systems to ensure that technological progress benefits society while addressing ethical concerns and maintaining public trust. As AI becomes integrated into economic activities, governance processes, and everyday life, questions regarding accountability, transparency, and responsible innovation have become increasingly significant.

Artificial intelligence can be broadly understood as the capability of machines to perform tasks that normally require human intelligence, including learning, reasoning, and decision-making. Another perspective describes AI as a system's ability to achieve defined goals across varied and dynamic environments. Both interpretations highlight AI's transformative potential while also raising economic, social, and ethical concerns about its widespread adoption.

In the contemporary digital era, technology has become deeply embedded in business operations, public administration, and daily social interactions. Consequently, the risks associated with AI extend beyond technical challenges and include broader societal implications such as privacy violations, algorithmic bias, economic disruption, and cybersecurity threats. Addressing these concerns requires the development of governance frameworks capable of balancing innovation with accountability and ethical oversight.

One important application of AI in governance is predictive analytics. Data-driven analytical tools allow governments to anticipate social risks, identify emerging livelihood needs, and allocate resources more effectively. During the COVID-19 pandemic, for example, data systems supported large-scale welfare initiatives such as free ration distribution and targeted financial assistance. These initiatives demonstrate how AI-enabled governance can improve administrative efficiency and responsiveness.

Governments worldwide are gradually transitioning from traditional administrative models—largely based on historical records, expert judgement, and manual analysis—to more data-driven governance systems. In this transformation, artificial intelligence functions not only as a technological tool but also as a strategic institutional mechanism that reshapes policy design and service delivery.

This study focuses primarily on the **technical and organizational dimensions of AI adoption within the public sector**, rather than on citizen perceptions or public attitudes toward these technologies.

II. DIGITAL INDIA: TECHNOLOGY, ARTIFICIAL INTELLIGENCE, AND GOVERNANCE

India's Digital India initiative has accelerated the development of digital infrastructure, internet connectivity, and technology-driven governance systems. Digital platforms now support essential services including financial transactions, government administration, and communication networks. As a result, artificial intelligence and digital technologies have become central components of national development strategies.

However, the rapid expansion of digital ecosystems has also increased exposure to cyber threats. As more services migrate to digital platforms, cybersecurity governance has become a critical priority for governments and institutions.

Recent statistics illustrate the rising scale of cybercrime in India. According to official data from the National Cyber Crime Reporting Portal (NCRP), reported cybercrime incidents increased from **1,029,026 cases in 2022 to 2,268,346 cases in 2024.** This rapid growth reflects the increasing vulnerabilities associated with widespread internet access and digital financial transactions.

The economic consequences of cybercrime have also become substantial. Government reports indicate that **Indian citizens collectively lost approximately ₹22,845 crore to cyber fraud in 2024,** demonstrating the significant

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

financial risks associated with digital platforms. These figures suggest that cybercrime now represents a systemic threat to the digital economy rather than isolated incidents.

To address these risks, the Government of India has introduced several policy and institutional measures to strengthen cybersecurity infrastructure. The **Union Budget 2025–2026 allocated around ₹782 crore for cybersecurity initiatives**, highlighting the government's commitment to strengthening digital security mechanisms.

Operational measures have also been implemented to disrupt cybercrime networks. Authorities have reportedly **blocked more than 942,000 SIM cards and 263,348 IMEI numbers** associated with fraudulent activities. In addition, the **national cybercrime helpline 1930** allows victims of online financial fraud to report incidents quickly and potentially prevent further losses.

The **Department of Telecommunications (DoT)** has also introduced the **Financial Fraud Risk Indicator (FRI)** framework. This system categorizes suspicious mobile numbers into risk levels such as Medium, High, and Very High, enabling telecom operators and financial institutions to detect and block potentially fraudulent communications.

Overall, the Digital India programme illustrates the dual nature of technological transformation: while digital technologies enhance efficiency and connectivity, they also generate new security challenges that require coordinated regulatory frameworks and institutional responses.

Table 1 | Growth of Cybercrime Incidents in India

Year	Reported Cybercrime Cases	Percentage Increase
2022	1,029,026	---
2023	1,596,493	55.15%
2024	2,268,346	42.08%

Source: National Cyber Crime Reporting Portal (NCRP), Ministry of Home Affairs.

III. TRACKING CYBER FRAUDS

Cyber fraud has evolved into a transnational phenomenon. Organized criminal networks operate across borders, frequently coordinating through digital communication channels and financial platforms. Some investigations have revealed large-scale operations sometimes referred to as "fraud factories," where organized groups conduct scams targeting victims across multiple countries.

IV. EMERGING CYBER THREATS

Recent technological developments have created new forms of cybercrime:

1. **AI-driven deepfakes and phishing:** Artificial intelligence can generate realistic audio, video, and image content that can be used to impersonate individuals or institutions in sophisticated fraud schemes.
2. **Misuse of digital payment platforms:** Systems such as the Unified Payments Interface (UPI) have expanded financial inclusion but are also exploited for unauthorized transactions, identity fraud, and social engineering scams.
3. **Illicit digital enterprises:** Cybercriminals often operate unauthorized online betting platforms and fraudulent digital applications that facilitate financial crime and money laundering.

V. DATA BREACHES

A data breach occurs when confidential or personal information is accessed or disclosed without authorization. As organizations increasingly rely on digital storage systems, such incidents have become more frequent and widespread.

One of the largest global breaches occurred during the **2025 "credentials crisis,"** which reportedly **exposed over 16 billion user records** containing passwords and login credentials. The breach affected accounts associated with major technology companies including Google, Facebook, Apple, GitHub, and Microsoft.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

Several high-profile incidents highlight the growing risks associated with data security. In **2018, India's Aadhaar biometric database** experienced a **leak** through a state-owned utility organization. In **2023, the Indian Council of Medical Research (ICMR)** suffered a breach affecting approximately **815 million COVID-19 testing records.** Earlier, in **2021, personal data belonging to 533 million Facebook users across 106 countries was leaked** on online forums.

These cases demonstrate the urgent need for stronger cybersecurity practices, improved data governance, and more robust encryption mechanisms.

Table 2: Major Cyberattacks in India

No.	Organization	Year	Type of Incident
1	Aadhaar UIDAI	2018	Biometric database breach
2	State Bank of India	2019	Banking data leak
3	BharatPay	2022	Financial platform hack
4	Swachhta Platform	2022	Government portal breach
5	AIIMS	2022	Healthcare cyberattack
6	RailYatri	2022	Data breach
7	Zivame	2022	E-commerce data leak
8	ICMR	2023	Health data breach
9	Sun Pharma	2023	Corporate cyberattack
10	Telangana Police Hawk Eye App	2023	Government application breach
11	NDMA	2023	Data leak
12	WazirX	2024	Cryptocurrency exchange breach
13	BSNL	2024	Telecom data breach
14	Energy Sector Targets	2024	Infrastructure cyberattacks

Source: Compiled from cybersecurity reports.(Sattrix Information Security.)

Common cybercrimes in India include phishing, ransomware attacks, identity theft, online scams, and data breaches.

VI. DATA BREACH PATTERNS AND RISK FACTORS IN INDIA

The number of data breaches continues to increase globally and within India. Several recurring vulnerabilities contribute to these incidents.

One significant weakness involves **inadequate API and endpoint security**. Many digital systems lack effective authentication, authorization, and rate-limiting mechanisms, enabling attackers to access sensitive databases.

Another common vulnerability involves **legacy infrastructure**. Older systems often operate with outdated software and insufficient security updates, making them attractive targets for cybercriminals.

Pattern Summary:

Older system → High vulnerability → Actively exploited by hackers

Why India Is an Attractive Target

Several structural factors contribute to India's exposure to cyber threats:

VII. INTERNATIONAL AI GOVERNANCE PRINCIPLES

AI governance frameworks aim to ensure the responsible design and deployment of artificial intelligence systems.

I. Real-World Applications

AI governance principles are increasingly applied across sectors:

1. **Banking:** Fairness and transparency in credit scoring models
2. **Healthcare:** Regulation of diagnostic AI tools and patient data protection

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

3. **Government:** Ethical use of AI in surveillance and service delivery
4. **Insurance:** Monitoring automated claim processing systems
5. **E-commerce:** Preventing algorithmic bias in pricing and recommendations

II. AI-Driven Decision-Making

AI supports improved decision-making through predictive analytics, data-driven policy development, and scenario modelling.

III. Resource Optimization

AI technologies also improve resource allocation through smart infrastructure planning, disaster management systems, and predictive maintenance of public assets.

IV. Drivers of AI Governance

The expansion of AI governance is influenced by increasing regulatory oversight, rapid enterprise adoption, rising expectations for transparency, and integration with governance, risk, and compliance frameworks.

VIII. ETHICAL CHALLENGES IN AI GOVERNANCE

The widespread adoption of AI introduces several ethical challenges.

Lack of transparency in algorithmic decision-making may obscure accountability for errors or discriminatory outcomes. AI systems trained on biased datasets can generate unfair results, raising concerns regarding equity and fairness. Privacy and data protection risks also increase as large volumes of personal data are processed.

Public trust is another critical factor. Citizen participation and transparency are essential for building confidence in AI-driven governance systems. Furthermore, regulatory frameworks often struggle to keep pace with technological change, creating legal uncertainties related to liability and intellectual property.

Finally, the **digital divide between urban and rural** regions may limit equitable access to AI-enabled services. Addressing these issues requires collaborative governance approaches that involve governments, private organizations, and civil society.

IX. GOVERNANCE FRAMEWORK FOR DIGITAL SECURITY IN INDIA

India has established several legislative and institutional mechanisms to strengthen cybersecurity governance. Key initiatives include the **Information Technology Act (2000),** the **IT Intermediary Rules (2021),** and the **Digital Personal Data Protection Act (2023).**

Institutional bodies such as **CERT-In**, the National Critical Information Infrastructure Protection Centre **(NCIIPC)**, and the **Indian Cybercrime Coordination Centre (I4C)** play essential roles in monitoring cyber threats and coordinating responses.

Additional initiatives include the **National Cyber Crime Reporting Portal,** the **Cyber Crime Prevention Against Women and Children Scheme,** the **Cyber Crisis Management Plan,** and analytics platforms such as **Samanvaya** for interstate cybercrime investigations.

Collectively, these initiatives represent a **multi-layered cybersecurity governance framework** designed to strengthen digital resilience and protect citizens.

X. AI GOVERNANCE IN INDIA: CHALLENGES AND OPPORTUNITIES

AI adoption in India presents both opportunities and challenges. Issues such as algorithmic bias, privacy risks, transparency gaps, and regulatory limitations require careful policy attention.

Despite these concerns, AI offers significant economic potential. Government projections estimate that **AI could contribute approximately $957 billion to India's GDP by 2035.** Global investment in AI is also expanding rapidly, reflecting the growing importance of AI technologies.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, June 2026 Impact Factor: 8.2

However, governance mechanisms remain limited. While AI investment is expected to grow significantly, only **20% of AI initiatives address governance and ethical considerations,** and just **5% of organizations report advanced governance maturity**.

XI. AI GOVERNANCE AS A PERFORMANCE DISCIPLINE

Many organizations treat AI governance primarily as a compliance requirement. However, effective governance frameworks can also enhance organizational performance and strategic value.

Organizations with mature governance structures benefit from improved sourcing strategies, stronger partner ecosystems, enhanced compliance, and greater operational efficiency. Data-driven assessments such as **AI maturity indices** can help organizations evaluate workforce readiness and manage AI transformation effectively.

XII. CONCLUSION

Artificial intelligence and digital technologies are reshaping governance, economic systems, and social interactions. While these technologies offer significant opportunities for innovation and development, they also introduce new cybersecurity and ethical challenges.

India's rapidly expanding digital ecosystem has improved connectivity and economic participation but has also increased exposure to cybercrime and data breaches. Strengthening cybersecurity infrastructure, improving regulatory frameworks, and promoting digital awareness are essential for building resilient digital systems.

As the world moves toward AI-driven economies, organizations and governments that adopt robust governance frameworks will be better positioned to ensure responsible innovation, protect citizens, and maintain public trust.

REFERENCES

1. Cybercrime statistics reported through the National Cyber Crime Reporting Portal (NCRP). Government of India. | Ministry of Home Affairs. (2025)
2. Citizens lost over □22,845 crore to cyber criminals in 2024 | Business Standard PTI. (2025).
3. India's cybercrime reporting systems logged over 22.7 lakh cases in 2024 | TOI (2025).
4. Cybercrime surge: India's digital growth shadowed by a rising fraud wave | IndiaTracker. (2025).
5. Indian Journal of Law and Legal Research Volume VIII Issue I | ISSN: 2582-8878
6. An Analytical Study of Cyber Law and Legal Framework in India | Mar-Apr 2025 IJIRMPS | ISSN: 2349-7300
7. CIGI | Digital Governance in 2026: The Key Shifts Shaping Technology, Security and Global Power
8. The impact of artificial intelligence on government digital service capacity | International Review of Economics & Finance | Volume 102, September 2025, 104374
9. The potential of an artificial intelligence (AI) application for the tax administration system's modernization: The case of Indonesia | Artificial Intelligence and Law, 31 (3) (2023), pp. 491-514
10. Tech Remediation | Artificial Intelligence in Governance: Enhancing Decision-Making in the Digital Age
11. Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review.
12. IBM Research. (2021). Trustworthy AI: The Role of Governance in AI Systems.
13. United Nations. (2021). Roadmap for Digital Cooperation: Implementation of the Recommendations of the High-Level Panel on Digital Cooperation.
14. IIPA Publications | Ai for Sushasan / AI in Governance: Risks and Challenges
15. ISG Research, The Sourcing Solution Platform | The Governance Gap
16. Ventana Research – Data Governance Benchmark Research
17. Governance of Generative AI | Policy and Society, Volume 44, Issue 1, January 2025,

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, June 2026
Impact Factor: 8.2

18. International Journal For Multidisciplinary Research E-ISSN: 2582-2160 | Artificial Intelligence and India's Emerging Role in Global Digital Governance
19. Sattrix Information Security.| List Biggest Cyber Attack in India
20. Curbing Cyber Frauds in Digital India | PIB Oct, 2025.