International Journal of Advanced Digital Systems
and Multidisciplinary Studies (IJADSMS),
Vol. 1, Issue 1, pp. 35–37, (2026)
Published: January 2026

Cyber Law and Digital Governance in India: Challenges and Emerging Trends

Mr. Ajit Kumar[1], Mr. Abhishek Kumar[2], Ms. Lakshmi Kumari[3], Mr. Sachin Kashyap[4], Ms. Kumari Puja[5]
[1]Assistant Professor, Amity Institute of Information Technology (AIIT), Amity University Jharkhand, Ranchi
[2,3,4,5]Assistant Professor ,School of Computer Applications, Noida Institute of Engineering and Technology (NIET) Greater Noida
akumar7@rnc.amity.edu[1],abhishek.kumar@niet.co.in[2],lakshmikumari.mca@niet.co.in[3], sachin.kashyap@niet.co.in[4]
kumari.puja@niet.co.in[5]

Abstract
This paper provides a comprehensive analysis of the intricate landscape of cyber law and digital governance within India, exploring the multifaceted challenges and dynamic emerging trends shaping the nation's digital future. It delves into the legal frameworks, policy gaps, and technological advancements impacting data protection, cybersecurity, and citizen privacy in the context of India's rapidly expanding digital ecosystem. Specifically, it examines the escalating prevalence of cybercrime and the complexities associated with electronic evidence, alongside the constitutional implications of digital rights and the imperative for robust cybersecurity measures in an era of e-governance. Furthermore, this study evaluates the evolving regulatory responses to these challenges, including discussions around parliamentary oversight for new provisions and alternative investigative mechanisms that respect fundamental rights. The analysis underscores the critical need for a multi-stakeholder approach to address vulnerabilities in digital infrastructure and safeguard democratic institutions against escalating cyber threats.

k**eywords**: cybercrime, electronic evidence, digital rights, data privacy, cybersecurity, digital governance, India.

Introduction
The rapid expansion of the digital economy in India, characterized by burgeoning e-commerce and extensive digital governance initiatives, necessitates a robust and adaptive legal framework to address emergent challenges in cybersecurity and data protection [1]. This digital revolution, while fostering significant societal and economic transformations, simultaneously exposes critical vulnerabilities within India's cyber ecosystem [2]. The increasing reliance on technology across vital sectors such as banking, healthcare, and public administration has amplified the risks of sophisticated cyber-attacks and data breaches, posing significant threats to individuals, businesses, and national security [3]. This escalating digital threat landscape underscores the urgent need for comprehensive cyber laws and effective digital governance strategies to safeguard sensitive information and maintain public trust in the digital realm [2]. A comprehensive legal framework is essential to address the complex issues arising from advanced cybercrimes, the integration of artificial intelligence, and the intricacies of cross-border data flows [4]. Moreover, the dynamic nature of cyber threats and the rapid pace of technological advancements, particularly in artificial intelligence, continually challenge the adequacy of existing legal provisions, often rendering them obsolete before full implementation [3]. Consequently, the legal infrastructure must evolve preemptively to regulate novel technological applications and secure digital sovereignty, particularly in areas like AI integration, which introduces unique regulatory dilemmas concerning accountability and oversight [5]. This is further complicated by the fact that many current laws are ill-equipped to handle the complexities introduced by AI, especially concerning issues like algorithmic bias and automated decision-making [6]. This gap highlights the necessity for a legal framework that balances technological advancement with robust protection for individual rights, particularly the right to privacy [7]. The absence of explicit data protection legislation until recently further exacerbated these vulnerabilities, leaving a significant regulatory void that cybercriminals exploited [8]. However, recent legislative efforts, such as the introduction of the Digital Personal Data Protection Act, aim to rectify this, establishing clearer guidelines for data handling and accountability [9]. This evolving regulatory environment, coupled with the persistent threat of sophisticated cyberattacks, underscores the critical need for continuous adaptation and enhancement of cyber law and digital governance mechanisms in India to effectively counter emerging digital threats and secure its rapidly expanding digital infrastructure [10], [11].

Literature Review
This section critically examines existing scholarship on India's cyber law and digital governance, identifying gaps in current research and establishing the foundation for a comprehensive analysis of challenges and emerging trends within this dynamic field [12]. The review synthesizes key findings from various studies, categorizing the identified lacunae and proposing potential pathways for improvement within India's cybersecurity framework [2]. Specifically, prior research often highlights the evolving nature of cyber threats and the inherent lag in legal adaptation, demonstrating how traditional legislative approaches struggle to keep pace with rapid technological advancements [13]. This disparity is particularly evident in the context of artificial intelligence, where the absence of a horizontal AI law in India leaves significant regulatory gaps, especially concerning AI-specific operational incidents like algorithmic bias and performance degradation [6], [14]. These complexities, particularly around algorithmic accountability and data privacy, reveal that the Information Technology Act of

2000 was not designed to address the nuances of advanced AI technologies, thereby weakening India's legal regime and threatening individual rights [6]. Furthermore, despite the enactment of policies like the National Cyber Security Policy 2013, India continues to grapple with an escalating number of cyber threats, ranking among the top ten countries most affected by cyberattacks in 2023 [2]. This persistent vulnerability underscores the inadequacy of current legal and policy frameworks in effectively mitigating sophisticated cyber warfare tactics and data breaches [15], [16]. The fragmented nature of India's legal landscape, encompassing various acts not specifically designed for contemporary cyber threats, further complicates the assignment of liability and effective enforcement in critical sectors like aviation cybersecurity [17]. This institutional fragmentation and lack of specific sectoral policies contribute to ambiguities in liability allocation and hinder robust enforcement mechanisms, especially when compared to international best practices [17]. Moreover, the absence of a centralized authority to coordinate cybersecurity efforts across diverse sectors exacerbates these challenges, leading to fragmented responses and inconsistent application of legal provisions [2]. This fragmented approach, particularly evident in areas like aviation cybersecurity, often results in critical oversight voids and ambiguous accountability for cyber incidents, impeding effective incident response and enforcement across different agencies [17].

Methodology

To address these gaps, this study employs a mixed-methods approach, combining doctrinal analysis of legislative frameworks with empirical investigation into their practical application and effectiveness. Specifically, a qualitative analysis will be conducted, drawing upon secondary sources such as legal texts, government publications, and scholarly discussions to assess India's regulatory stance against international frameworks and best practices [17]. This qualitative approach will involve a comparative analysis of India's cyber law landscape with regulatory models adopted by the European Union, the United States, and China, particularly concerning AI governance and data protection [18]. This comparative lens will highlight strengths and weaknesses in India's current legal architecture and identify areas where legislative enhancements are necessary to align with global standards and adequately address emerging cyber threats [3], [17]. The research will also incorporate a detailed examination of case studies involving significant cyber incidents in India to evaluate the practical implications of existing laws and identify areas where enforcement mechanisms need strengthening [17]. Furthermore, the study will analyze expert opinions and policy recommendations to provide a holistic understanding of the challenges faced by law enforcement agencies and suggest pragmatic solutions for capacity building and inter-agency coordination [19]. This comprehensive approach aims to provide actionable insights for policymakers to develop more resilient and adaptable cyber legal frameworks, ensuring India's digital security in an increasingly interconnected world. Additionally, the methodology encompasses a systematic review of academic literature to synthesize existing knowledge on cybercrime, digital threats, and policy implications within the Indian context, thereby identifying prevalent trends and persistent challenges [2].

Results

The preliminary findings suggest that while India possesses a foundational legal framework for cybersecurity, its reactive nature and lack of granular specificity for advanced technologies like AI create significant vulnerabilities [20]. This includes an inadequate focus on privacy rights, as the Information Technology Act of 2000 primarily facilitated e-commerce without prioritizing robust data protection mechanisms [21]. This oversight underscores a critical need for comprehensive legislation that explicitly addresses data privacy, aligning with global standards and recognizing the right to privacy as a fundamental digital age entitlement [22]. The current regulatory landscape, characterized by sector-specific frameworks, falls short in establishing a unified and comprehensive approach to AI governance, particularly when compared to more integrated models found in the European Union [18]. This fragmented approach, coupled with overlaps and ambiguities across various laws, creates significant compliance challenges for stakeholders and often leads to confusion regarding legal obligations and enforcement [3]. Furthermore, the analysis reveals that despite an increase in cybercrime cases, the reporting mechanisms are often inadequate, and law enforcement agencies face challenges due to a lack of specialized knowledge and resources to effectively investigate and prosecute cyber offenses [23], [24].

Discussion

These challenges are exacerbated by the rapid evolution of cyber threats, which consistently outpace the development and implementation of new legal and technological countermeasures, thereby necessitating a proactive and adaptive regulatory posture [25]. This requires a departure from the current reactive legal framework towards one that anticipates future cyber risks and integrates advanced technological solutions, such as AI-driven threat intelligence, into its core design [21], [26]. The absence of a dedicated, comprehensive AI law in India, unlike the European Union's robust regulatory framework, creates a significant legislative gap that raises concerns about market disruptions and ethical oversight [18]. This regulatory void is further complicated by the lack of clear guidelines for algorithmic accountability and data privacy within AI applications, which can lead to significant vulnerabilities and erode public trust [6]. The Information Technology Act of 2000, while foundational, is primarily focused on e-commerce and cybercrime, leaving significant gaps in comprehensive data protection and privacy, a deficiency often highlighted when compared to international data protection statutes [8], [27].

Conclusion

This inadequacy underscores the urgent need for India to develop a robust, forward-looking legal framework that can effectively address the multifaceted challenges posed by emerging technologies and evolving cyber threats, ensuring both national security and individual rights in the digital age. Such a framework would ideally incorporate proactive measures for data protection, mirroring the comprehensive approach seen in developed nations, rather than relying on disparate contractual agreements for data safeguarding [21]. Indeed, the existing legal instruments, including the Information Technology Act of 2000 and the Contract Act of 1872, offer only partial coverage for data protection, highlighting the necessity for dedicated legislation to safeguard personal information [21]. This includes the development of a comprehensive data protection law that aligns with international standards, such as the General Data Protection Regulation, which emphasizes strong user rights and corporate accountability [3]. The recent enactment of the Digital Personal Data Protection Act 2023 represents a crucial step in addressing these lacunae, aiming to provide a more resilient legal framework for data governance that matches the accelerating pace of technological evolution,

including advancements in generative AI and quantum computing [28].

References

[1] A. Patil, “Navigating the Digital Landscape: India’s Evolving Legal Framework for E-commerce, Data Protection, and Cyber security,” SSRN Electronic Journal , Jan. 2024, doi: 10.2139/ssrn.4850285.

[2] A. Chakraborty and S. Tiwari, “An analytical study on challenges and gaps in India’s cyber security framework,” International Journal of Criminal Common and Statutory Law , vol. 5, no. 1, p. 4, Jan. 2025, doi: 10.22271/27899497.2025.v5.i1a.110.

[3] M. Gupta and A. Gupta, “Cyber Security Legal Framework in India – Overlaps, Problems and Challenges,” Journal of Business Management and Information Systems , vol. 12, no. 1, p. 11, Mar. 2025, doi: 10.48001/jbmis.1201002.

[4] A. Lamba, P. N. Nayyar, and T. Tanwar, “Cybersecurity Laws and Privacy Protection in India,” in Advances in Social Science, Education and Humanities Research/Advances in social science, education and humanities research , 2025, p. 22. doi: 10.2991/978-2-38476-426-6_3.

[5] T. Meghwal, “Emerging Challenges in Regulating Artificial Intelligence Under Cyber Security Laws in India,” Jan. 2025, doi: 10.2139/ssrn.5030258.

[6] S. A.V. and N. D. N. -, “Legal Challenges of Artificial Intelligence in India’s Cyber Law Framework: Examining Data Privacy and Algorithmic Accountability Via a Comparative Global Perspective,” International Journal For Multidisciplinary Research , vol. 6, no. 6, Nov. 2024, doi: 10.36948/ijfmr.2024.v06i06.31347.

[7] N. Joshi, “Emerging Challenges in Privacy Protection with Advancements in Artificial Intelligence,” International Journal of Law and Policy , vol. 2, no. 4, p. 55, Apr. 2024, doi: 10.59022/ijlp.171.

[8] N. Deo and P. A. Singh, “Cybersecurity and Sustainable Development,” 2022, p. 188. doi: 10.55662/book.2022ccrs.009.

[9] J. Foram, “Cybercrimes and the Legal Framework of India,” Zenodo (CERN European Organization for Nuclear Research) , Oct. 2025, doi: 10.5281/zenodo.17588657.

[10] L. Qudus, “Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges,” International Journal of Science and Research Archive , vol. 14, no. 1, p. 1146, Jan. 2025, doi: 10.30574/ijsra.2025.14.1.0225.

[11] S. K. Pittala, “Cybersecurity and Online Safety: A Critical Asset in the Information Era,” Journal of Frontiers in Multidisciplinary Research , vol. 4, no. 1, p. 576, Jan. 2023, doi: 10.54660/.jfmr.2023.4.1.576-579.

[12] D. Lata and RajVardhan, “An Analytical Study of Cyber Law and Legal Framework in India,” International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences , vol. 13, no. 2, Apr. 2025, doi: 10.37082/ijirmps.v13.i2.232693.

[13] O. O. Amoo, A. Atadoga, T. O. Abrahams, O. A. Farayola, F. Osasona, and B. S. Ayinla, “The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system,” World Journal of Advanced Research and Reviews , vol. 21, no. 2. GSC Online Press, p. 205, Feb. 08, 2024. doi: 10.30574/wjarr.2024.21.2.0438.

[14] A. Agarwal and M. J. Nene, “Incorporating AI Incident Reporting into Telecommunications Law and Policy: Insights from India,” 2025, doi: 10.48550/ARXIV.2509.09508.

[15] S. Sahak, R. Rajamanickam, and M. S. Hassan, “Liability of internet intermediaries and legal challenges: a comprehensive systematic review,” Quality & Quantity , Sep. 2025, doi: 10.1007/s11135-025-02344-y.

[16] K. Gaur, R. Chakraborty, G. Khemani, K. Sharma, and M. K. Jangid, “A Review on Cybersecurity Law and Management,” Lecture notes in networks and systems . Springer International Publishing, p. 341, Jan. 01, 2024. doi: 10.1007/978-981-99-9043-6_28.

[17] M. O. Farooqui, A. Sarhan, and F. Mustafa, “Aviation Cyber Security in India: Legal Gaps, International Frameworks, and Policy Reforms,” Yustisia Jurnal Hukum , vol. 14, no. 2, p. 186, Sep. 2025, doi: 10.20961/yustisia.v14i2.101653.

[18] N. Basu and R. Dave, “Comparative Analysis of Laws in AI,” Journal of Lifestyle and SDGs Review , vol. 5, no. 3, Feb. 2025, doi: 10.47172/2965-730x.sdgsreview.v5.n03.pe05575.

[19] N. M. Dr. J. A. Masudi, “CYBER SECURITY AND DATA PRIVACY LAW IN PAKISTAN: PROTECTING INFORMATION AND PRIVACY IN THE DIGITAL AGE,” Pakistan Journal of International Affairs , vol. 6, no. 3, Sep. 2023, doi: 10.52337/pjia.v6i3.906.

[20] A. Sharma, S. Sharma, S. D. Soni, P. Agrawal, P. K. Mishra, and G. Mourya, “Artificial Intelligence in the Indian Criminal Justice System: Advancements, Challenges, and Ethical Implications,” Journal of Lifestyle and SDGs Review , vol. 5, no. 1, Jan. 2025, doi: 10.47172/2965-730x.sdgsreview.v5.n01.pe04877.

[21] V. Singh and D. R. Gautam, “Cyber Crime, Security and Regulation in India,” 2022, p. 147. doi: 10.55662/book.2022ccrs.005.

[22] N. Mittal and G. Kaur, “A Comprehensive Socio-Legal Analysis Of Cybercrime In India: Patterns, Challenges, And Legal Frameworks,” International Journal of Environmental Sciences , vol. 11, p. 923, Jun. 2025, doi: 10.64252/1mv9w160.

[23] M. Manjunath and D. S. S, “A Study on Cyber Frauds Post Digitalization in India,” International Journal for Research in Applied Science and Engineering Technology , vol. 12, no. 4, p. 1790, Apr. 2024, doi: 10.22214/ijraset.2024.60191.

[24] G. Makam, “Cybercrime and Electronic Evidence in India: a Comprehensive Analysis,” SSRN Electronic Journal , Jan. 2023, doi: 10.2139/ssrn.4475784.

[25] N. AllahRakha, “Transformation of Crimes (Cybercrimes) in Digital Age,” International Journal of Law and Policy , vol. 2, no. 2, Feb. 2024, doi: 10.59022/ijlp.156.

[26] Y. Fernandes and N. Abosata, “Analysing India’s Cyber Warfare Readiness and Developing a Defence Strategy,” arXiv (Cornell University) , Jun. 2024, doi: 10.48550/arxiv.2406.12568.

[27] T. Satpathy, “The Aadhaar: ‘Evil’ Embodied as Law,” Health and Technology , vol. 7, no. 4, p. 469, Jul. 2017, doi: 10.1007/s12553-017-0203-5.

[28] A. K. Jha, “The Changing Face of the Data Protection Laws: From India’s IT Act to Global Privacy Standards,” African Journal of Biomedical Re