Page 2944 - 2954 **DOI:** *https://doij.org/10.10000/IJLMH.116470*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 6

2023

Indian Cyber Act: Lacunae and Recommendations

PRANAV PRAKASH[1], SURBHI GIRDHAR[2] AND ANTONY JOSE[3]

ABSTRACT

The evolution of cyber law in India is not merely a legislative process but a strategic imperative that impacts national security, economic stability, and the privacy rights of its citizens. Therefore, the collective efforts of lawmakers, cybersecurity experts, and the international community are essential in shaping a future where digital advancements and security go hand in hand. The study critically analyses the Indian Information Technology Act, 2000 (IT Act), assessing its effectiveness against the evolving cybercrime landscape and its adequacy in protecting data in the digital age. The scope encompasses thoroughly examining the Act's provisions and amendments, evaluating India's cybercrime trends and how the Act stands up to new-age cyber threats, and comparing with global data protection laws to gauge international harmonisation. Moreover, the study investigates enforcement challenges, scrutinises the roles of the judiciary and law enforcement agencies, and identifies the lacunae in public awareness and education on cybersecurity. Based on these analyses, it proposes recommendations for policymakers, legal experts, and cybersecurity stakeholders engaged in fortifying the nation's digital defences.

Keywords: *IT Act, Cybersecurity, Cybercrime, Data Protection, Cyber Law.*

I. INTRODUCTION

Cybersecurity in India is not just a matter of national security, but it also underpins the economic and social fabric of the nation. The heightened cybersecurity concerns have placed enormous pressure on India's legal system to provide an effective mechanism for the prevention, investigation, and prosecution of cybercrimes (Choudhury, 2023). However, this rapid digitization has outpaced cybersecurity development, leading to a spike in cybercrimes. These incidents range from financial fraud and data theft to cyber espionage and attacks on critical infrastructure, which have significant repercussions on national security and public trust. According to the National Crime Records Bureau (NCRB), India has seen a sharp increase in

[1] Author is a Research Scholar at Department of Criminology, Karunya Institute of Technology and Sciences, Coimbatore, India.
[2] Author is an Assistant Professor at Department of Criminology, Karunya Institute of Technology and Sciences, Coimbatore, India.
[3] Author is a Research Scholar at Department of English, Karunya Institute of Technology and Sciences, Coimbatore, India.

 [ISSN 2581-5369]

cybercrime events; in 2019, there were 63.5% more cases reported than in 2018 (*Crime In India*, 2020). Consequently, the need for a comprehensive cyber law framework is imperative to safeguard national interests and align with global cybersecurity norms. India has witnessed a notable reduction in cybercrime with the enactment of the Information Technology Act and the granting of exclusive powers to law enforcement and other authorities to combat cybercrime. The powers of the human mind are beyond understanding. History demonstrates that no strategy has ever been able to eradicate crime worldwide entirely. The only ways to reduce crime are to strengthen the enforcement of existing laws and to educate people about their rights and obligations, which includes reporting crimes to society as a common responsibility (Patil, 2022).

The study critically analyses the Indian Information Technology Act, 2000 (IT Act), assessing its effectiveness against the evolving cybercrime landscape and its adequacy in protecting data in the digital age. The scope encompasses a thorough examination of the Act's provisions and amendments, an evaluation of India's cybercrime trends and how the Act stands up to new-age cyber threats, as well as a comparison with global data protection laws to gauge international harmonization. Moreover, the study investigates enforcement challenges, scrutinises the roles of the judiciary and law enforcement agencies, and identifies the lacunae in public awareness and education on cybersecurity. Based on these analyses, it proposes recommendations for policymakers, legal experts, and cybersecurity stakeholders engaged in fortifying the nation's digital defences.

II. INDIAN INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, of 2000 (IT Act), marked the commencement of dedicated cyber law in India. Enacted on October 17, 2000, it was a response to the United Nations Model Law on Electronic Commerce 1996, which recommended that all member states consider the model in the light of their legal systems (*UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996*, 1999). The IT Act was revolutionary as it recognized the validity of electronic records and digital signatures, which facilitated the legal infrastructure for e-commerce and e-governance (*The Information Technology Act*, 2000). Over the years, the IT Act underwent significant changes to address the complexities of evolving cyber threats. The 2008 amendment was particularly notable, expanding the scope of the Act to include new offences and strengthen the legal framework of data protection, privacy, and cybersecurity. It introduced Section 66A, which penalized sending offensive messages, and Section 69, "which granted powers to the government to intercept, monitor, or decrypt information generated,

 [ISSN 2581-5369]

transmitted, received, or stored in any computer resource" (*Information Technology (Amendment) Act*, 2008). Some of the key milestones in Indian cyber law post the enactment and amendment of the IT Act include the notification of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, which laid down specific guidelines for the protection of sensitive personal data, the Supreme Court of India's judgment in Shreya Singhal v. Union of India (2015), which struck down Section 66A of the IT Act as unconstitutional, citing concerns over freedom of speech, and the introduction of the Draft Personal Data Protection Bill in 2018, drawing inspiration from the GDPR, aimed to establish a comprehensive data protection regime in India.

The Act lays down the legal framework for electronic governance by giving recognition to electronic records and digital signatures (*The Information Technology Act*, 2000). It defines cybercrimes and prescribes penalties—ranging from damage to computer systems, unauthorized access, downloading, and fraud. The IT Act was amended in 2008 to introduce specific provisions for identity theft, cyber terrorism, and child pornography, among others, reflecting an attempt to address the evolving nature of cyber threats (*Information Technology (Amendment) Act*, 2008). Despite these amendments, the IT Act has been criticized for not keeping up with rapid technological changes and for its broad provisions that grant extensive power to government authorities without sufficient checks and balances. Section 43A and the IT Rules, 2011 under the Act prescribe compensation for failure to protect sensitive personal data, mandating corporate bodies to implement reasonable security practices (*The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules*, 2011). The Act covers a range of offences under Sections 65 to 67B, addressing data theft, identity theft, child pornography, and cyber-terrorism. A significant section is 43A, which deals with compensation for failure to protect sensitive personal data, and Section 72A, which provides for punishment for the breach of confidentiality and privacy (*Information Technology (Amendment) Act*, 2008). The IT (Amendment) Act 2008 introduced Section 66A (later struck down), Section 69 (giving authorities the power to intercept, monitor, or decrypt information), and Section 79 (related to intermediaries' liabilities). The IT Act's strength lies in its pioneering role in establishing a legal framework for electronic transactions and cybersecurity. It was one of the first legislations that recognized electronic contracts, thereby legitimizing e-commerce in India. By setting out penalties for cybercrimes, it laid the groundwork for legal recourse in cases of cyber offenses, which was absent in the traditional penal codes (Kashyap & Chaudhary, 2023). The Act also established the Indian Computer Emergency Response Team (CERT-In) as the national nodal agency for incident response,

 [ISSN 2581-5369]

thereby institutionalizing the process of cybersecurity management (*The Indian Computer Emergency Response Team (CERT-In)*, 2004).

III. Lacunae in Indian Cyber Act

In recent years, India has witnessed several significant cyber incidents that have raised concerns over the country's cybersecurity preparedness. One notable case was the Cosmos Bank heist in 2018, where hackers siphoned off nearly ₹94.42 crores through thousands of transactions across 28 countries within two hours ("Cosmos Bank's Server Hacked; Rs 94 Crore Siphoned off in 2 Days," 2018). Another incident involved a malware attack on the Kudankulam Nuclear Power Plant's administrative network in 2019, which was a stark reminder of the vulnerabilities in critical infrastructure These incidents, among others, highlight the sophisticated nature of cyber-attacks and the need for a robust response mechanism to detect, prevent, and respond to such threats effectively (Paliwal, 2019). The IT Act has provisions that address unauthorized access and data theft, but its effectiveness against new-age threats like ransomware, phishing, and sophisticated state-sponsored cyber espionage is questionable. The Act does not explicitly mention these modern forms of cybercrimes, leading to challenges in legal interpretation and enforcement. Moreover, the Act lacks specific provisions for emerging technologies such as the Internet of Things (IoT), artificial intelligence (AI), and blockchain, which are increasingly being exploited by cybercriminals (Alawida et al., 2022). The financial incentive for hackers is much bigger than the punishment, thus laws alone will not make them quit committing crimes. The best way for ordinary people to deal with these cyberattacks is to be aware of certain frequent attacks and how to prevent them, as technology will never be perfect or completely safe. Updates and secures for the system should be applied by users as soon as possible (Shaikh & Chudasama, 2021). The most difficult thing about cybercrime is that it's always changing; there is no set place or identity. The true identity of the cybercriminal is concealed from the outset of the crime. Therefore, cybercrime has to be treated with the same seriousness as other crimes in our society. The state of the cyber legal system today is still insufficiently advanced to stop the widespread cybercrime that is now taking place. The new type of cybercrime that is emerging as a result of growing technology is not even covered by regulation (Supriya et al., 2022).

There is still a list of violations that encourage abusers of computer-generated space since there are no severe consequences or punishments. For example, Spam is a major issue in today and the issue of spamming is not addressed in the IT Act of 2000 in any way. Phishing is the illicit practice of deceiving people to get sensitive personal information, such as credit card numbers,

 [ISSN 2581-5369]

passwords, and user names. This is an example of how the tactic known as 'social engineering' is used to trick consumers. The Information Technology Act, of 2000 does not contain any legislation about phishing; nonetheless, the term 'cheating' is mentioned throughout the IPC (Devi, 2019). The rapid advancement in technology often outpaces the amendments in the IT Act. For instance, the advent of cloud computing presents challenges in jurisdiction and data sovereignty that the Act does not address comprehensively. The increasing use of AI for both, attack and defence, creates a scenario where the existing legal framework may not be adequate to assign liability or protect against AI-powered threats. The absence of explicit guidelines on cybersecurity practices for emerging technologies is a significant gap that leaves stakeholders without clear legal directives.

The Act and its amendments address privacy concerns primarily under Section 43A and Section 72A. Section 43A holds the body corporate responsible for implementing and maintaining reasonable security practices and procedures to safeguard Sensitive Personal Data or Information (SPDI). It mandates compensation for any negligence in maintaining the requisite security standards leading to wrongful loss or gain. Section 72A provides for punishment for disclosure of information in breach of a lawful contract or without the consent of the information provider. While these sections provide a basis for data protection, critics argue that they are not comprehensive and do not cover the entire spectrum of data privacy. There are no clear guidelines for data processors or collectors on how to handle the data, and there is a need for a more robust mechanism to address data breaches. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, provides some standards for data protection. The IT Act's data protection provisions are less stringent than international privacy standards like the GDPR. The GDPR emphasizes the rights of individuals over their data, including the right to be forgotten, data portability, and strict consent requirements, which are not explicitly covered under the IT Act (*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Da*, 2016). There is also a lack of clarity in the IT Act regarding cross-border data transfers and data localization requirements, which are well-defined under the GDPR. Moreover, the GDPR mandates the appointment of a Data Protection Officer (DPO) and regular impact assessments, which are not required by the IT Act (Sen, 2021). To align with international privacy standards, India has proposed the Personal Data Protection Bill, which aims to establish a comprehensive data protection framework for India (*The Personal Data Protection Bill*, 2018).

 [ISSN 2581-5369]

Cybercrimes can be perpetrated from any location, creating complexities in determining the applicable jurisdiction and the enforcement of laws across different territories. The enforcement mechanisms under the IT Act are often constrained by the lack of Mutual Legal Assistance Treaties (MLATs) with other countries, which are crucial for cross-border cooperation in the investigation and prosecution of cybercrimes. Law Enforcement Agencies (LEAs) in India play a crucial role in implementing the IT Act. However, they often encounter various obstacles such as inadequate technical expertise, insufficient resources, and a lack of specialized cybercrime units. This impacts their ability to effectively investigate and prosecute cybercrimes (Singh, 2019). The National Cyber Crime Reporting Portal was launched as an initiative to facilitate victims/complainants to report cybercrime complaints online; however, the follow-up on these complaints requires strengthening the capacity of LEAs. Despite the IT Act's provisions, there is a general lack of awareness among the public about their rights and the mechanisms for redressal under the law. Educational initiatives and awareness campaigns are essential to empower netizens to protect themselves against cyber threats and to understand the legal remedies available to them.

IV. RECOMMENDATIONS FOR MORE EFFECTIVE CYBER ACT

To address the evolving nature of cyber threats, it is recommended that the IT Act be amended to provide clear definitions and comprehensive coverage of cybercrimes. This includes categorizing and defining modern threats such as ransomware, deep fakes, and IoT-based attacks. Ensuring that the language of the Act is precise can minimize ambiguities and facilitate better enforcement. The current penalties under the IT Act may not suffice as effective deterrents. It is recommended to revise the penalty structure to impose stricter fines and longer imprisonment terms for cybercrimes, particularly those affecting critical infrastructure and national security. Such enhancements should be benchmarked against the severity of offences to act as real deterrents. There is a need to integrate advanced threat response mechanisms, including real-time intelligence sharing, incident response protocols, and cyber forensics capabilities. Establishing a framework for these mechanisms would ensure a proactive and coordinated response to cyber incidents. The creation of an autonomous and specialized administrative authority for cyber issues is recommended. This body would oversee cybersecurity regulations, compliance, and enforcement, and would be responsible for coordinating with international cyber law enforcement for cross-border issues (Singh, 2019). The government should work towards standardizing cybersecurity practices across different industry sectors, especially for those handling sensitive personal data. This could involve mandatory cybersecurity audits, adherence to international cybersecurity standards, and

 [ISSN 2581-5369]

reporting mechanisms for data breaches (Slapničar et al., 2022). Public-private partnerships (PPPs) in cybersecurity should be promoted to leverage the strengths of both sectors. Such collaborations can lead to the sharing of best practices, pooling of resources, and joint initiatives for cybersecurity research and development (CERT-In, 2020).

International cooperation is paramount in the enforcement of cyber laws due to the global nature of the internet and cyber threats. Cybercrimes often transcend national borders, making it challenging for any single country to effectively tackle them without collaboration. India could benefit from engaging in mutual legal assistance treaties (MLATs), extradition treaties, and cooperative frameworks such as the Budapest Convention, which provides a comprehensive approach to cybercrime and electronic evidence (Council of Europe, 2001). Such international agreements and cooperation would facilitate the sharing of information, resources, and best practices, as well as aid in the investigation and prosecution of cross-border cybercrime. Policy harmonization involves aligning India's cyber laws with international standards to create a consistent legal environment that can protect against and respond to cyber threats effectively. This could include adopting definitions and standards that are in line with those used internationally. Furthermore, India should consider establishing a data protection authority, akin to those in European countries, to enforce data protection laws and oversee compliance with international standards. The proposed Personal Data Protection Bill, which is inspired by the GDPR, is a step in this direction (Ministry of Electronics and Information Technology, 2018). To facilitate harmonization, India could also actively participate in international discussions on cybersecurity, contribute to the development of global cyber norms, and ensure that these norms are reflective of the interests of diverse stakeholders, including developing nations.

V. CONCLUSION

The Indian Information Technology Act of 2000 stands as a pioneering legislative framework that has set the foundation for addressing cyber law in India. However, it faces significant challenges in keeping pace with the rapidly evolving digital threat landscape. The Act's provisions, while groundbreaking at the time of enactment, now require substantial updates to address the nuances of modern cyber threats, privacy concerns, and the integration of advanced technological developments. The critiques highlighted in this paper point to the need for clearer definitions, stronger enforcement mechanisms, enhanced penalties, and a comprehensive approach to data protection that is in line with international standards. The jurisdictional challenges and the imperative of cross-border cooperation underline the necessity for India to engage in global cyber law frameworks and harmonize its laws with international norms.

 [ISSN 2581-5369]

Recommendations for reform, including the establishment of a dedicated cyber administrative authority, standardizing cybersecurity practices across industries, and fostering public-private partnerships, are critical steps towards bolstering India's cybersecurity posture. Furthermore, public awareness and education remain key components in creating a resilient digital infrastructure that can safeguard against cyber threats. India's journey towards a robust cyber legal framework is ongoing. The proposed Personal Data Protection Bill is indicative of a forward-looking approach, and such legislative initiatives must be pursued with urgency. Harmonizing with international cyber law not only strengthens domestic cybersecurity but also positions India as a responsible and proactive member of the global digital community. The evolution of cyber law in India is not merely a legislative process but a strategic imperative that impacts national security, economic stability, and the privacy rights of its citizens. Therefore, the collective efforts of lawmakers, cybersecurity experts, and the international community are essential in shaping a future where digital advancements and security go hand in hand.

*****

 [ISSN 2581-5369]

VI. REFERENCES

- Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003
- Choudhury, C. (2023). *Cyber Security Concerns: A threat to India's National Security*. Modern Diplomacy. https://moderndiplomacy.eu/2023/02/17/cyber-security-concerns-a-threat-to-indias-national-security/
- Cosmos Bank's Server Hacked; Rs 94 crore Siphoned off in 2 Days. (2018, August 14). *The Economic Times*. https://economictimes.indiatimes.com/industry/banking/finance/banking/cosmos-banks-server-hacked-rs-94-crore-siphoned-off-in-2-days/articleshow/65399477.cms
- *Crime In India*. (2020). National Crime Records Bureau (NCRB). https://ncrb.gov.in/crime-in-india.html
- Devi, P. (2019). Cyber Laws in India: A Critical Analysis. *Think India Journal*, *22*(35), 1900–1906.
- *Information Technology (Amendment) Act*. (2008). Ministry of Electronics and Information Technology, Government of India. https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMTk4NzY=
- Kashyap, A. K., & Chaudhary, M. (2023). Cyber security laws and safety in e-commerce in India. *Law and Safety*, *89*(2), 207–216. https://doi.org/10.32631/pb.2023.2.19
- Paliwal, A. (2019, November 6). Had informed govt about Kudankulam nuclear power plant cyber attack: Former NTRO cyber security analyst. *India Today*. https://www.indiatoday.in/india/story/had-informed-govt-about-kudankulam-nuclear-power-plant-cyber-attack-former-ntro-cyber-security-analyst-1616304-2019-11-06
- Patil, J. (2022). Cyber Laws in India: An Overview. *Indian Journal of Law and Legal Research*, *4*(1), 1391–1411. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4049059
- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da*.

 [ISSN 2581-5369]

(2016). European Parliament, & Council of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj

- Sen, P. (2021). EU GDPR and Indian Data Protection Bill: A Comparative Study. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3834112
- Shaikh, N. G., & Chudasama, D. (2021). Research on Cyber Offenses under Information Technology Act, 2000. *Recent Trends in Parallel Computing*, *8*(1), 14–20. https://www.researchgate.net/publication/351955175_Research_on_Cyber_Offenses_under_Information_Technology_Act_2000
- Singh, R. K. (2019). The Information Technology Act 2000: A Scientific Review. *Anusandhaan-Vigyaan Shodh Patrika*, *7*(1), 82–86. https://www.anushandhan.com/index.php/ANSDHN/article/view/1291
- Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. *International Journal of Accounting Information Systems*, *44*, 100548. https://doi.org/10.1016/j.accinf.2021.100548
- Supriya, R., Tomar, K. P., Singh, K., Bhardwaj, M., & Tyagi, S. (2022). Cyber Crimes in India: A Critical Analysis. *International Journal of Mechanical Engineering*, *7*(6), 304–312. https://kalaharijournals.com/resources/JUNE-27.pdf
- *The Indian Computer Emergency Response Team (CERT-In)*. (2004). Ministry of Electronics & Information Technology, Government of India. https://www.cert-in.org.in/PDF/RFC2350.pdf
- *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules*. (2011). Ministry of Electronics and Information Technology, Government of India. https://www.indiacode.nic.in/handle/123456789/1362/simple-search?query=The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.&searchradio=rules
- *The Information Technology Act*. (2000). Ministry of Law and Justice, Government of India. https://lddashboard.legislative.gov.in/actsofparliamentfromtheyear/information-technology-act-2000
- *The Personal Data Protection Bill*. (2018). Ministry of Electronics and Information Technology, Government of India. https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

 [ISSN 2581-5369]

- *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996*. (1999). United Nations. https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce

*****

 [ISSN 2581-5369]