

ABHIDHVAJ LAW JOURNAL

[www.abhidhvajlawjournal.com]

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Editor In chief – Assistant Professor Mr. Janmejay Singh

Publisher & Founder – Vaibhav Sangam Mishra

Frequency – Quarterly (4 Issue Per year)

ISSN: 2583-6323 (Online)

Copyright © 2025 - 26

CYBERSECURITY LAWS IN INDIA- OUTDATED?

AUTHOR'S NAME – Akshit Dev Singh, B.A.LL.B, Second Year.

INSTITUTION NAME – Symbiosis Law School, Nagpur.

Received on 18 June 2025, Accepted on 20 June 2025, Published on 7 July 2025

ABSTRACT:

In this world where almost everything revolves around technology, and technology is rapidly advancing at a very fast rate, these advancements have made our lives easier. It has given rise to cybersecurity issues and various cyberattacks. This paper will discuss the state of cybersecurity in India and the legal framework related to it, like the Information Technology Act 2000 and the more recent Digital Personal Data Protection Act, 2023. While the Information Technology Act deals with cyber-related issues but it has become outdated over a period of time, and this paper highlights new threats like AI-driven attacks, multi-stage intrusions, and ransomware, and IT Act inefficiency handling these cases. This paper also talks about India's cooperation globally and how it has helped build international relations with other countries. This paper also highlights the importance of a more unified and dynamic approach to cybersecurity, like emphasizing the importance of modernizing laws, enhancing capacity building. This paper argues that a robust and adaptive cybersecurity is required for India to safeguard its digital future, protect its citizens, etc.

1) INTRODUCTION:

In today's rapidly growing world, cybersecurity has become a concern of prime concern, as cyber threats are becoming more prevalent in society, and it is further continuing to evolve, posing significant risks to national security, economic stability, and individual privacy. There are several threats in this era of digital technologies, like data breaches, ransomware attacks, and espionage campaigns. India, as one of the largest and fastest-growing economies, plays a crucial role in international cybersecurity initiatives. In the history of the Internet, no cyberattack is known to have killed a human being, but this attack is more dangerous than any biowar as it disrupts the flow of the country. No country has declared cyberwar or even admitted to sponsoring a cyberattack. Nevertheless, the damage caused by human malice is

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

enhanced by digital capabilities far exceeding expectations[1]. India's international cybersecurity strategy does not limit itself to the domestic sphere, and as we know that India has the third largest internet user base in the world, estimated at around 200 million, and is expected to grow more rapidly. As Prime Minister Narendra Modi pointed out in his speech at the BRICS Summit in Brazil, India considers cyberspace to be a source of great opportunity but cybersecurity to be an equally great concern. The government is looking to cyberspace as the main medium to improve and empower citizens through various e-governance schemes, as well as creating feedback mechanisms[2]. India has also taken several initiatives and introduced many laws related to cybersecurity like The **Information Technology Act, 2000** (often referred to as the IT Act) is the primary legislation in India that addresses legal aspects of cybersecurity, cybercrime, and e-commerce. The IT Act provides legal recognition for electronic contracts, regulates digital signatures, and defines offenses such as hacking, identity theft, and cyber terrorism. It also includes provisions for the establishment of the **Cyber Appellate Tribunal**[3]. Although this act deals with various cyber-related issues, it is outdated as it does not include new cybercrimes like ransomware attacks, deepfakes, and AI-generated content crimes etc. Different types of information sharing can be used to improve cybersecurity in various ways. By sharing threat perceptions and national policies, states can better understand each other's concerns and priorities. By conducting multilateral exercises and sharing best practices for the protection of networks, critical infrastructure, and software/hardware, states can help each other ensure safe data transfer across borders[4]. There are several cybercrimes going on, and there are very less provisions available to tackle these crimes. There is a need for the formation of international organizations to tackle these crimes. These crimes vary from distributing malware to phishing and keylogging (PwC 2011). Several authors have shown that cybersecurity measures are becoming necessary in managing cybercrimes (*Vande Putte & Verhelst, 2013; Pilling, 2013; von Solms & van Niekerk, 2013). Wolfpack (2012)* stated that

[1] Dobbins, J., Solomon, R. H., Chase, M. S., Henry, R., Larrabee, F. S., Lempert, R. J., Liepman, A. M., Martini, J., Ochmanek, D., & Shatz, H. J., Cybersecurity. In *Choices for America in a Turbulent World: Strategic Rethink*, RAND Corporation (June 20, 2025, 8:00 P.M.) https://www.rand.org/pubs/research_reports/RR1114.html.

[2] Samuel, C., D. D. Cheong (Ed.), *Cybersecurity: Some Critical Insights and Perspectives*, S. Rajaratnam School of International Studies (June 20, 2025, 8:00 P.M.), https://rsis.edu.sg/rsis-publication/rsis/cybersecurity-some-critical-insights-and-perspectives/.

[3] Government of India, https://www.meity.gov.in/sites/default/files/IT%20Act%202000.pdf (last visited on June 20, 2025).

[4] Hitchens, T., & Goren, N. (2017). *International Cybersecurity Information Sharing Agreements*. Center for International & Security Studies (June 20, 2025, 8:00 P.M.), https://cissm.umd.edu/sites/default/files/2019-07/Cyber%20information%20sharing%20agreement%20report%20-%20102017%20-%20FINAL.pdf

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

effectively managing cybercrimes would involve the creation of cybersecurity institutes, a comprehensive national cybersecurity structure, and cybersecurity response teams[5].

Research Questions

1. How efficient are the Information Technology Act 2000 and Digital Personal Data Protection Act 2023 in tackling emerging problems like AI-driven attacks, multi-stage intrusions, etc.?
2. To what extent does limited technical expertise and limited law enforcement training hinder proper management of cybersecurity, and what measures should we take to improve it?
3. In what ways can India build international relations that can help in the improvement of the cybersecurity sector in India, and what steps has India already taken to foster a unified national approach?

2) CYBER SECURITY LAWS AND POLICIES IN INDIA:

2.1 Information and Technology Act, 2000 (IT Act):

The Information and Technology Act, 2000, is the most crucial cybersecurity act, and initially, it was enacted to facilitate electronic commerce and digital governance. This act has undergone several changes to help manage growing cyber fraud. This act provides a legal framework to address problems like cybercrimes, digital signatures, electronic contracts, digital signatures and e-governance. Specific provisions handle crimes like **hacking (Section 66)**[6], **identity theft (Section 66C),**[7] and **cyberstalking (Section 66A)**[8]. These types of acts are very important not only in India but all over the world, as cybercrimes have been on the rise at a rapid rate. Undoubtedly, the criminal class has taken up the new at a much greater speed than our lawmakers and law agencies. It has startled the world as much as the Inter amazed them. In 1888, an inspector was quoted in the Chicago Herald affirming "a well-known fact that no other section of the population avails itself more readily and speedily of the latest triumphs of science

[5] Enigbokan, O., & Ajayi, N. (2017). Managing Cybercrimes Through the Implementation of Security Measures. *Journal of Information Warfare*, Journal of Information welfare (June 20, 2025, 8:00 P.M.) https://www.jinfowar.com/journal/volume-16-issue-1/managing-cybercrimes-through-implementation-security-measures.

[6] Information Technology Act, 2000, No. 21 of 2000, 66, Act of Parliament (India).

[7] Information Technology Act, 2000, No. 21 of 2000, 66C, Act of Parliament (India).

[8] Information Technology Act, 2000, No. 21 of 2000, 66A, Act of Parliament (India).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

than the criminal class".1 Can there be a greater truth as far as the Internet is concerned?[9] Although the Information and Technology Act deals with several problems related to cybersecurity but there is a need for several amendments to make it functional with modern problems, and this Act was last amended in 2008, which shows how outdated this Act is.

2.2 The Digital Personal Data Protection (DPDP) Act, 2023:

The Digital Data Protection (DPD) Act, 2023, is India's first encompassing legislation, and its main aim is the protection of personal data. It aims to balance an individual's rights with data privacy and explain the role of government intervention in the data privacy of an individual. The acts govern the processing of digital personal data within India, including the data that is collected online or offline and subsequently digitized. It also expands outside India if it involves offering goods and services within the country.[10]. This act also stipulates a fine of up to 250 crores for bodies failing to protect digital data or misusing information.[11]. The DPDP Act,2023, demonstrates a critical shift in India's Protection landscape, aligning with global standards like the European Union's General Data Protection Regulation (GDPR)[12]. There is a necessity to implement more acts like this to prevent any mishappening, and there are several cases in which we have seen more acts like these. We can take the example of the case SR *Siras v. Aligarh Muslim University.*[13] In this case, SR Siras, who was a reader and chair of Modern Indian Languages of Aligarh Muslim University, filed a writ petition against Aligarh Muslim University in Allahabad High Court as In February 2010, some members of the press broke into his residential quarters and filmed him having sex with another male. On the next day, the Vice Chancellor of the University placed the petitioner under suspension and ordered him to vacate his house. This was clearly a violation of his rights relating to privacy and equality. This case reflects how there is an urgent need for new innovations and schemes to protect the personal data of citizens.

[9] Bharuka, D. (2002). INDIAN INFORMATION TECHNOLOGY ACT, 2000 CRIMINAL PROSECUTION MADE EASY FOR CYBER PSYCHOS. *Journal of the Indian Law Institute* (June 20, 2025, 8:00 P.M.) https://www.jstor.org/stable/43951825.

[10]PRS Legislative Research. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (last visited on June 20, 2025).

[11] Data Protection Bill, https://www.business-standard.com/topic/data-protection-bill (last visited on June 20, 2025).

[12] European Union. (2016). https://eur-lex.europa.eu (last visited on June 20, 2025).

[13] Dr. Shrinivas Ramchandra Siras & Ors. v. The Aligarh Muslim University & Ors. (2010). Civil Writ Petition No. 17549 of 2010. Allahabad High Court.

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

2.3 Bharat National Cybersecurity Exercise (Bharat NCX 2024):

The Bharat National Cybersecurity Exercise is an initiative launched by the government and was inaugurated in New Delhi, and multiple stakeholders, including government agencies and private sector leaders, participated in it[14]. The exercise emphasized cross-sector collaboration, including CERT-In, the *Ministry of Electronics and Information Technology (MeitY)*, and *the National Critical Information Infrastructure Protection Centre (NCIIPC)*[15]. Advanced simulations targeted vulnerabilities in IT and OT systems, reflecting the increasing complexity of cyber threats globally.[16]. These types of policies play an important role in helping common people become conscious of cybercrimes and help them to report these types of criminal activities to the concerned authorities. As we know that cybercrimes are more prevalent in developed countries like the USA, etc. Compared to developing countries like India. A final reason why cybercrimes are likely to differ in developing and developed countries is related to cognitive factors. Cyber-criminals and victims in developing countries are likely to differ in their cognitive assessment of crimes as well as in confidence, skill, and experience.[17].

3) CHALLENGES IN INDIA's CYBERSECURITY FRAMEWORK:

3.1) Fragmented Legislation:

India's cyberlaw framework is primarily governed by the Information Technology Act, 2000 (IT Act), which was last amended in 2008. While the IT Act addresses various cybercrimes, including hacking, identity theft, and cyberterrorism, it is widely considered outdated and inadequate to tackle the complexities of modern cyber threats[18]. The existing legal regime in India adopts a fragmented and piecemeal approach towards cybersecurity and data privacy. This fragmentation leads to challenges in enforcement and compliance, as businesses and individuals must navigate a complex web of regulations without a unified legal framework[19]. This type of legislation will stagnate India's growth and will hinder India's potential to become

[14] Desk, O., & Ciso, E., Bharat NCX 2024 inaugurated, to strengthen cyber defense, strategic decision-making. *ETCISO* (June 20, 2025, 8:00 P.M.) https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/bharat-ncx-2024-inaugurated-to-strengthen-cyber-defense-strategic-decision-making/115418580.

[15] *Ministry of Electronics and Information Technology,* https://www.meity.gov.in/ (last visited on June 20, 2025).

[16] *Computer Emergency Response Team*, https://www.cert-in.org.in/ (last visited on June 20, 2025).

[17] KSHETRI, N., Diffusion and Effects of Cyber-Crime in Developing Economies. JSTOR (June 20, 2025, 8:00 P.M.) https://www.jstor.org/stable/27896600.

[18] Bytescare, https://bytescare.com/blog/challenges-to-indian-law-and-cybercrime (last visited on June 20, 2025).

[19] *Legal Developments*, https://www.legal500.com/developments/thought-leadership/cybersecurity-laws-in-india-is-it-time-for-a-regime-change/ (last visited on June 20, 2025).

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

a developed country. This can also lead to increased crime rates, and because of this, the whole country can fall into chaos. So, there is a need for more advanced legislation and more amendments to the current constitution of India. There should be more awareness camps related to cybercrimes, as it will help people to understand more about these crimes, and it can also help to reduce cybercrimes significantly in India. The government should implement more schemes like Cyber Swachhta Kendra, which is an initiative that focuses on detecting and removing malicious botnet programs from computers and devices. It provides free tools for malware analysis and helps improve the security of systems and devices[20].

3.2) Capacity constraints:

There is limited technical expertise, and law enforcement agencies often lack the necessary training and skills to tackle these types of crimes. For instance, in 2011, the Delhi Police Cybercrime Cell had only two inspectors, and there were reports of improper evidence collection due to inadequate training. The Indian government's limited resources impede the development and enforcement of cybersecurity regulations and standards. This scarcity affects the establishment of a robust cybersecurity infrastructure and the implementation of comprehensive. The rapid growth of India's IT and business process management sectors has led to increased pressure from international clients and governments to strengthen cybersecurity measures. However, balancing these demands with domestic economic constraints remains a challenge[21]. Because of these conditions, India is unable to solve several problems like poverty, unstable economy, and unemployed youth, and this gives cybercriminals a golden opportunity, as unemployed youth who are unable to find a job often fall into the trap of these fraudsters to earn easy money but end up losing their own money. The government should introduce more jobs related to this field, as it will also help the unemployed youth to get a new job and stop being liabilities for their country, and it will also lead to an increase in efficiency and will prevent cybercrimes from happening and will also lead to a more stable economy of the country. Kaushik Ray, Co-Founder & COO, WhizHack Technologies, shares a ringside view of the cybersecurity industry in India and the job market pertaining to it. He said, "*We have a popular saying in our office when we hear of layoffs by*

[20] Cybersecurity Centre of Excellence (CCoE). https://ccoe.dsci.in/blog/the-role-of-government-initiatives-in-tacklingcybersecuritychallengesinindia#:~:text=National%20Cybersecurity%20Policy%3A%20The%20National,information%20and%20other%20critical%20infrastructure. (last visited on June 20, 2025).

[21] Kshetri, N. (2015). India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership. *IEEE Security & Privacy*, https://doi.org/10.1109/msp.2015.61 (June 20, 2025, 8:00 P.M.)

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

the gigantic stalwarts like Google, Facebook, Microsoft, etc. The saying is 'Layoffs or Payoffs?' Cybersecurity has joined the traditional recession-proof professions like Medicine and Education, as Cybersecurity is increasingly becoming a basic human necessity, if not a human right"[22].

3.3) New evolving threats:

In India cybersecurity aspect is growing at a very fast rate, and there are also several threats growing with it, and some of them are-

1. **Attacks using AI-** There is a rapid increase in cybercriminals who are using AI for their benefit. They are using large, modified software that uses AI to corrupt any software, and they are also undetectable. This includes complex phishing emails and adaptive malware[23].
2. **Multi-channel and multi-stage attacks-** With evolving technologies, threats are becoming more complicated, like breaking into one platform and expanding to others, and manipulating security gaps in interconnected devices and fragile identity measures[24].
3. **Ransomware surge-**India has witnessed a rapid 150% increase in ransomware attacks, and there are several organizations that are paying huge ransoms. There are various attackers who use triple and double extortion tactics, including ransomware[25].
4. **Advanced Persistent Threats (APTs)-**There are also several state-sponsored threats that include highly skilled attackers, and they are also well-versed in AI. They are usually hired for stealthy operations to target sensitive information, which poses significant threats to government agencies and major industries.

ABHIDHVAJ LAW JOURNAL

[22] India, T. O., Cybersecurity job market remains resilient despite economic downturn. *The Times of India*. (June 20, 2025, 8:00 P.M.) https://timesofindia.indiatimes.com/top-headlines/cybersecurity-job-market-remains-resilient-despite-economic-downturn/articleshow/98848751.cms.

[23] Ciso, E., Cybersecurity threat trends that will impact Indian businesses in 2025, Barracuda highlights. *ETCISO.,*(June 20, 2025, 8:00 P.M.) https://ciso.economictimes.indiatimes.com/news/next-gen-tech/cybersecurity-threat-trends-that-will-impact-indian-businesses-in-2025-barracuda-highlights/116461082

[24] *Id* at 2344.

[25] Anand, V., Cybersecurity Awareness Month 2024: Organisations must revamp defences against evolving threats, says Deloitte. *CNBCTV18*(June 20, 2025, 8:00 P.M.), https://www.cnbctv18.com/technology/cybersecurity-awareness-month-2024-organisations-must-revamp-defences-against-evolving-threats-says-deloitte-partner-19494537.htm

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

These threats can harm a country in several ways and can also initiate wars between countries. There are very limited provisions to tackle these types of threats, and these types of threats are emerging all over the world. There are several cases in which various companies have created AI-generated images of various celebrities, which have harmed their privacy. One of these several cases is *Anil Kapoor v. Simply Life India & Ors.*[26] In which Anil Kapoor who is a famous Indian actor filed a complaint against company named Simply Life India because they were using his image, voice and other attributes using **AI** for their commercial gain and this case clearly highlighted that how dangerous can **AI** be and it can be used to create deepfakes of any person and how it can also be used against that person. This case was set as a landmark judgement in which the High Court of Bombay declared its decision in favour of Anil Kapoor and highlighted the rights of celebrities in the Digital Age, and it also set a precedent for cases involving the mix of technology, media, and intellectual property.

CONCLUSION:

In the end we can say that India is having a very rapidly evolving digital landscape, so it requires well organized laws and schemes to prevent the country from felling into chaos, and it will also indirectly improve overall growth of the country as technology will be put into a good use and by strict laws we can prevent misuse of any technology and it will also lead to decrease in the rate of cybercrime. We can recognize cyberspace as an immense opportunity, but it also gives rise to great concerns. India's Cybersecurity laws mainly include laws related to the Information Technology Act 2000, which has been supported by newly introduced frameworks like the **Digital Personal Data Protection Act 2000**[27] and initiatives such as **Bharat NCX**[28]. While these initiatives demonstrate that India is slowly moving to a more secure digital environment but there are several challenges that still exist. The nature of India's framework is very limited, and the limited experts in this field makes it very difficult to manage cybercrimes. Furthermore, there are several threats that are evolving rapidly, like AI-powered attacks, multi-stage intrusions, ransomware surges, and sophisticated Advanced Persistent

[26] Ahmed, A. S. (1992). Bombay Films: The Cinema as Metaphor for Indian Society and Politics, JSTOR (June 20, 2025, 8:00 P.M.), https://www.jstor.org/stable/312677.
[27] PRS Legislative Research. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (last visited on June 20, 2025).
[28] Desk, O., & Ciso, E., Bharat NCX 2024 inaugurated, to strengthen cyber defense, strategic decision-making. *ETCISO*(June 20, 2025, 8:00 P.M.) https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/bharat-ncx-2024-inaugurated-to-strengthen-cyber-defense-strategic-decision-making/115418580

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Threats that constantly challenge today's defense system. To strengthen India's defense system, it is essential to focus on certain aspects like modernizing and unifying legislation, enhancing capacity building and skill development, fostering public-private partnerships and information sharing, prioritizing awareness and education, and strengthening international cooperation. By improving these aspects in the Indian system, it can build a more organized and proactive cybersecurity framework in India. It can also prevent cyberwarfare in the nation and between different nations.

ABHIDHVAJ LAW JOURNAL

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.