

Cybercrime 2.0: Evolving Digital Threats and The Indian Legal Framework

Balajeyasakthi J *

* Student, LL.M., (Cyber Law), School of Law, Joy University, Tirunelveli, Tamil Nadu, India

Review Article History

Received: 03-Oct-2026
Revised: 07-Oct-2026
Accepted: 09-Oct-2026
Published: 12-Oct-2026

Keywords

Artificial Intelligence
Cybercrime 2.0
Cybersecurity
Data Protection
Digital Evidence
Indian Cyber Law
Online Fraud

Abstract

The fast growth of technologies has resulted in the development of cybercrimes into technologically complex forms of crimes that go beyond the conventional crimes like unauthorised access and data breach. In fact, the emergence of artificial intelligence, deepfakes, cryptocurrency, connected devices and social engineering is seen as the emergence of Cybercrime 2.0 that is discussed in the current paper. India, as one of the largest digital economies in the world, is faced with a challenge to address the constantly evolving cyber-threats. As for the mechanisms to combat cyber-crime, there is the legislative and institutional framework based mainly on the Information Technology Act, 2000, and supplemented by Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023. However, the rate of technological advancement is usually faster than legislative and institutional response. The following research paper sheds light upon the evolving concept of Cybercrime 2.0 and the ability of India's legal system to meet the challenges of new threats in the digital age. Specifically, such problems as jurisdiction, digital evidence, attribution, enforcement, platform protection and individual rights protection will be considered. The paper emphasizes the need for a comprehensive legislative approach based not only on the expansion of criminal offenses but also on the development of flexible legislation, better investigation methods and institutions.

Corresponding Author:

Balajeyasakthi J

Student, LL.M., (Cyber Law), School of Law, Joy University, Tirunelveli, Tamil Nadu, India
balajeyasakthi@gmail.com

This article is under the [CC BY- NC-ND](#) licenses
Copyright @ Journal of Law and Legal Research
Development, available at www.jllrd.com



1. INTRODUCTION

The fast growth of the digital age has had an effect on the way people interact, do business, avail themselves of public facilities and handle their financial affairs. In India, the increase in the use of smartphones, digital payments, cloud computing, social networking sites and the use of public infrastructure in the digital domain have made the country a very highly connected digital environment. The above-mentioned change has brought many benefits to society and economy but at the same time has offered new opportunities for committing criminal acts. Cybercrime is no longer limited to the crime against computers and computer networks. Criminal acts are increasingly being committed using digital tools, automation and artificial intelligence. Cybercrime has therefore been significantly redefined in its very nature. The past iterations of cybercrime were largely associated with criminal acts like

unauthorised access, spread of malware, attacking websites and theft of digitally stored information. However, the current offenders take advantage of human behaviour, online identity, technology weaknesses and fast-growing computational methods. Criminal acts can be organized from afar, automated on a massive scale and aimed at victims in various jurisdictions. Such phenomenon can thus be called "Cybercrime 2.0" or a more advanced stage of cybercrime where technology is not just used for committing a crime but is also used for planning, performing, scaling and concealing the act. The importance of Cybercrime 2.0 is not only due to the emergence of novel methods of crime but also due to the challenge in using conventional laws for dealing with technology-based offenses. Issues relating to criminal liability, attribution, jurisdiction, electronic evidence, and investigations become more complex with the offenders conducting their operations through

anonymous accounts, manipulated digital identity, automated systems, or infrastructure existing in different jurisdictions. On the other hand, the victim suffers financial losses, damage to reputation, mental anguish, invasion of privacy, or being exploited via technology for a long period of time. A fairly significant legal and institutional regime has been developed in India to deal with crimes relating to cyber offences. Among them, the Information Technology Act, 2000 serves as the primary legal instrument covering various forms of computer-based criminal activities, while the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023 serve as wider laws for criminal procedure and evidence relating to the commission of crimes through digitally facilitated means. There have also been advances in relation to data protection and cybersecurity regulation, among other areas of development in the regulation of cyber offences. However, it must be noted that the existence of laws in itself is no assurance that there will be an effective response to technologically advanced crime. Hence, the question which drives this research paper is whether India's current legal framework is capable of adjusting to the nature of evolving cybercrime. This entails examining not just individual types of crimes but rather the evolution of digital criminal activity in general. The paper concludes that regulation of Cybercrime 2.0 should not be confined to the introduction of new offenses and severe penalties. Successful regulation depends on the combination of technology-friendly legislation, competent investigative agencies, trustworthy systems for gathering digital evidence, cooperation of all involved parties and privacy protection measures. An innovative approach to the regulation of cybercrimes in the future is needed in order to make sure that the existing framework of cyber-law in India will continue being efficient without compromising the essential legal norms in pursuit of the digital security.

2. CONCEPTUALISING CYBERCRIME 2.0

Cybercrime evolved as technology developed. Initially, cybercrime referred only to illegal activities involving computers, computer systems and information in electronic format. As digital technologies came to form an integral part of our life, the scope of criminal activity extended beyond attacks on technological facilities. Criminals started using online identity, communications and other technological means and resources to achieve their goals. The current state is another step in evolution, when new technologies may accelerate the speed, size and complexity of criminal activity. The paper applies the term "Cybercrime 2.0" to the current environment. Cybercrime 2.0 is not automatically classified as another category of crimes. It is rather a model of development, which illustrates how current criminal activities are changing under the influence of advanced technologies. The key difference between traditional cybercrimes and Cybercrime 2.0 lies in the increasing role played by the connection between technology, human psychology, and criminal intentions. A cybercriminal might use not only his technical skills but also manipulations, automation of attacks, and information from the Internet for carrying out an attack. Therefore, success can largely depend on human psychology rather than breaking some technical security measures. The main feature of Cybercrime 2.0 is its increased scalability. Usually, any crime has its limits in terms of geography, manpower, and time it takes to approach a victim one by one. But the presence of digital technologies makes such limitations much smaller. Only one scam, malicious software, and even compromised account can be enough to reach a large

audience in a short amount of time. Besides, automation allows conducting more crimes while not personally participating in them. Adaptability is yet another feature that can be attributed to cybercrimes. These criminals have the capacity to change their tactics quickly due to the technological innovations as well as any changes in security and behaviour on the users' side. When the previous tactic fails, alternative strategies can be developed quite swiftly. Another thing to be mentioned is that cybercriminals may make use of legitimate internet-based services in order to disguise their crimes, thus making it even harder to distinguish a crime from regular internet use. Another distinctive feature of Cybercrime 2.0 is that there is a blurring line between cyber-dependent and cyber-enabled crimes. In fact, cyber-dependent crimes are those which cannot be committed without using digital technologies. As for cyber-enabled crimes, they include traditional criminal intentions being implemented with the help of digital technologies. However, things get complicated when a criminal scheme involves both technical hacking and regular deceit, fraud, impersonation or harassment. Another characteristic of the new cybercrime is its increasing transnational character. The crime may be committed by someone in one country, with the help of infrastructure based in another country, targeting victims in multiple countries, with proceeds being transferred internationally via digital financial transactions. Thus, the physical distance may not impede the offender's access to the victim. However, the investigators are still confined to operate within the territorial confines of the criminal justice process and the limitations of territorial legal systems and procedures. The discrepancy between the borderless nature of the digital world and the territorial nature of criminal law is the key problem of Cybercrime 2.0. The concept also embodies the rising role of the personal information available via digital means. Personal information can be used to create an artificial identity, to target certain people and to communicate fraudulently. On the other hand, the digital footprint can help the offender as well as the investigator. The same digital environment that enables criminals to hide their identity may at the same time produce information that could help establish the pattern of behaviour, communication and finances. Cybercrime 2.0 is thus an evolution from considering cybercrime as merely the illegal disruption of computer-based systems to considering crime in an increasingly networked world. The key features of cybercrime 2.0 are adaptability, scalability, automation, manipulation of human behaviour, being transnational, and the convergence of crimes. This is significant because laws created in response to past iterations of cybercrime may not be sufficient to address modern digital crimes. A comprehension of this change paves way for a discussion on the particular cybercrime threats that exist today.

3. MODERN FORMS OF CYBERCRIME IN THE DIGITAL ERA

The evolution of Cybercrime 2.0 can be seen in the growing array of digital threats. Criminals do not rely anymore on only one approach in gaining illegal access or doing harm. Rather, modern cybercrime involves both the use of technology and deception and the manipulation of human behaviour and digital financial systems. The examples below show how the cyber threat environment is evolving. One of the biggest threats is cybercrime with the help of artificial intelligence. Artificial intelligence can help criminals to produce realistic messages, find potential victims, automate some routine actions and adjust fake communications according to each specific target.

In addition, the technology can lower the level of knowledge necessary for carrying out certain illegal operations. In this way, the problem is not just the fact that criminals use a new technology, but the fact that technology can make more efficient and personalized the methods of crime. Deepfakes and synthetic media represent another big threat to national security. Artificially produced audio, video and image content can impersonate people and create fake communications. This can be applied for committing such crimes as impersonation, fraud, defamation, and spreading misinformation. With the rise in the quality of the synthetic media, there is also the issue of evidence. If there is the presence of digital recording, then it does not prove anymore the occurrence of an event. Social engineering has likewise progressed. There is increasing reliance on psychological persuasion techniques, apart from technical hacking, in phishing, smishing, and impersonation attacks. Psychological manipulation techniques include making the person feel the need for haste or fear to make him/her reveal information, transfer money, or grant access to his/her bank account. Information on personal life, revealed by a person on the Internet on social networking sites, could help convince the victim into giving in to the demands. Here, the person is targeted as a decision-making entity rather than as the one who uses an insecure system. One very worrying trend in India is the prevalence of “digital impersonation” and “digital arrest.” Criminals may pose as police or officials of any kind and threaten the victim with imaginary legal trouble. Here, the reason for success of these frauds lies in the combination of technological means of communication with psychological manipulation. Even ransomware and data extortion go beyond mere encryption. In contemporary attacks, an attacker might steal information from an organization and threaten to release the information publicly unless their demands are met. In such cases, an organization can suffer from operational disruption, financial losses, confidentiality issues, and reputational damage simultaneously. The growing reliance of companies and governmental organizations on digital networks increases vulnerability to cyber-attacks significantly. The rise of cryptocurrencies and online financial systems offers more ways for criminals to commit frauds. Digital currencies can be involved in various fraudulent activities including deceptive investments, fraudulent financial transactions, and money laundering. Online investment fraud might consist of social media marketing of the fake financial platform, the platform itself, and persuasive communications. Identity theft and account takeover have also taken on greater significance with the increasing importance of digital identity within finance, communication, commercial transactions and government service. The use of stolen information, tampered devices and fraudulent authentication attempts could potentially result in criminals gaining access to someone else’s account. The ramifications go beyond any initial financial damage since the stolen identity could then be used for committing additional crimes. Digital technology has also made stalking, harassment and image-based abuse easier to perpetrate. The persistent communication features, anonymity and the ability to quickly disseminate digital content could allow perpetrators to continue intimidating and humiliating their victims. This kind of abuse does not stop even once the original content is deleted, as digital content can easily be replicated and shared by others. The other vulnerability that comes with the increase in the usage of IoT devices and technologies is that smart devices, connected cars, home security, and even industrial technologies will become targets if not sufficiently protected. A hacked device can act as a doorway into a larger system or as a tool for

a broader hack attack. With the increased integration of physical infrastructure with digital technology, there are more implications to cybercrime than just losing information and finances; physical safety can also be at stake. As illustrated above, emerging cybercrimes are not just about the technology itself but about the interplay between technological capabilities and human vulnerability to such technologies. The diversity of such crimes requires a legal approach that would address such conduct which may not fall under any category of crime traditionally known before. This leads us to the following section, which will explore how the legal approach in India addresses the challenges mentioned above.

4. LEGAL REGULATION OF CYBER CRIME IN INDIA

The legislative approach adopted by India towards cybercrime has been formulated in light of a number of measures, including cyber-specific legislation, criminal laws, processual provisions, provisions for the admissibility of electronic evidence and institutional arrangements. This is on account of the realization that certain forms of illegal activity in relation to the use of digital technology cannot be dealt with under one act only. The Information Technology Act, 2000 continues to be the key legislation addressing different types of unlawful activity using computers. The IT Act 2000, also known as the Information Technology Act, is the statutory law governing the prosecution of cybercrimes in India. This Act recognises electronic records and transactions and has legal consequences of various types of illegal acts committed via computers or information in electronic form. Sections on unauthorised access, destruction of computer resources, identity crimes, cheating by using electronic communications, invasions of privacy and cyber terrorism offer different legal approaches to tackle the technology crime problem. There are other sections in the Act dealing with the liabilities of intermediaries and power of the government in connection with certain digital activities. The Bharatiya Nyaya Sanhita, 2023 (BNS) is significant in relation to cybercrime since a number of crimes committed via digital platforms will still fall within the ambit of general principles of criminal law. Crimes such as fraud, cheating, criminal intimidation, forgery, stalking, defamation, among others, can be committed using electronic communication or digital platforms. Using technology does not necessarily mean that the crime committed is exempted from the ambit of general criminal law. Hence, the BNS is complementary to the IT Act in relation to conduct having aspects of both digital and conventional crimes. The procedural law will be contained in the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS). In the course of investigating cybercrimes, there will be seizing of electronic devices, gathering of digital information, examining witnesses, searches, arrests, and cooperation among investigative authorities. Procedural law becomes critical when the electronic evidence is located at various places or even controlled by third parties. Therefore, successful investigation relies on not only the substantive laws but also on proper procedures. The importance of Bharatiya Sakshya Adhiniyam, 2023 (BSA) in the sphere of digital crime is highlighted because current investigations rely heavily on electronic records. In this respect, messages, emails, documents on a computer, CCTV footage, phone logs, server data, transaction records and other forms of digital evidence become crucial to establish an offence. The system of evidences is a system that is legally allowed to treat electronic and digital records in

accordance with the law of evidence. This requires that all electronic data should be reliable, authentic, and properly preserved. The problem of cybercrimes in India is solved not only through the legislative framework but also through specific institutions. The Indian Computer Emergency Response Team (CERT-In) is an important tool to deal with any problems related to cyber incidents and coordination in such matters. The National Cyber Crime Reporting Portal enables citizens of India to report about certain cybercrimes whereas cybercrime police units and other investigative institutions deal with criminal investigations. Digital financial institutions are important participants in this regard. There is also regulation that has been put in place in the form of data protection and digital governance. The Digital Personal Data Protection regime is intended to regulate the processing of digital personal data and also create obligations related to its processing. Even though there are differences between data protection law and criminal law, they have a point of interaction where the misuse or unauthorized disclosure or compromise of the personal information leads to illegal activities. This is why data governance is an important part of the legal context in which modern cyber threats have been regulated. Another area that India has recognized as being important is the issue of intermediary liability and platform governance. The digital platforms play an important role since the communications, user accounts, financial transactions, and digital content often traverse private networks. There are specific legal obligations imposed by the legal regime on the intermediaries, and also there are certain conditions applicable to them in terms of their legal protection and obligations. Thus, the Indian system can be seen as a multi-tier legal system where the IT Act has specific cyber provisions, the BNS contains broader provisions dealing with criminal activity, the BNSS has mechanisms of investigation and procedures to follow, the BSA deals with the rules regarding the evidence, including digital, while specialized bodies and digital governance contribute to it as well. This means that the law is able to tackle cybercrime using various legal and institutional approaches. Nevertheless, presence of several legal instruments is not enough in itself to ensure proper response to the rapidly changing cyberspace. Divergence between the speed of technological advances and corresponding law, problems related to the attribution and jurisdiction, increased complexity of electronic evidence and limited capabilities for investigations give rise to some serious doubts. They need to be critically considered rather than just listed. The next chapter will consider major legal and enforcement issues related to Cybercrime 2.0.

5. LEGAL AND ENFORCEMENT PROBLEMS

There are many tools in the Indian legal system to deal with cybercrime, but the quick pace at which new forms of cybercrime appear creates obstacles which cannot be overcome through legislation alone. The main issue here is the gap between the pace of technological advancement and the much slower pace of changes to laws, institutions and investigation practices. Consequently, cybercrime 2.0 highlights some of the problems not necessarily due to the absence of laws in India, but the way in which these laws can be applied. The first problem is related to technological neutrality and adaptability of the law. The criminal practices can change dramatically within a short time period, while any amendments to statutory laws are subject to long legislative procedures. A legal framework, closely linked with specific technologies, can

become less efficient once these technologies develop or become obsolete. Therefore, future-looking cyber legislation has to be able to regulate any criminal behaviour without being tightly connected with technical terms. The issue of attribution is yet another serious problem. It might turn out to be harder to identify the person responsible for committing the cybercrime than to prove that it took place. Offenders could carry out their criminal acts via hacked accounts, anonymizers, fictitious identities or facilities owned by other persons. Different persons might also take part in various stages of the criminal act. Thus, investigators should be able to make a definite link between the digital act and the person supposed to commit it. Furthermore, the international nature of the crime causes certain jurisdiction problems. The digital evidence could be hosted in one country, owned by the firm residing in the other and associated with the offender who works somewhere else. In such situations, cooperation with other countries or international service providers would be necessary on the part of investigative bodies. This, however, could take time and make certain investigative powers less effective. The other significant consideration relates to digital evidence. Digital evidence can be easily destroyed, manipulated, encrypted or moved from one system to another. It becomes necessary to determine its authenticity and chain of custody from the time of collection up until it reaches the courtroom. This becomes difficult with the increasing prevalence of artificial intelligence and synthetic media, as the digital evidence that may seem convincing could have been manipulated. Legal standards and expertise become essential for both courts and investigators to be able to separate authentic from fake digital evidence. Capacity becomes another important factor that needs to be considered. Investigation of cybercrimes demands specialized knowledge in computer networks, digital forensics, fintech, encryption, and data analysis among others. The investigative capacity varies among different investigating teams. The increased participation of private digital platforms and services providers poses yet another problem. Information may be possessed by social media companies, cloud service providers, telecoms, banks and any other private entity. Investigation could require access to that information following the rules of law and in a reasonable time frame. Any delays with regard to securing and disclosing the information might result in loss of its evidential significance, which might have been crucial for determining the identity of the perpetrator. Another issue related to cybercrimes is privacy protection. Increased powers of investigation will assist in better detection and investigation of offenses, but an overreaching surveillance may impede privacy and other civil liberties. A lot of personal information may be collected during digital investigations that goes far beyond the scope of the crime itself. The key question then is how to ensure that any cybersecurity measure is reasonable, lawful and justified. Under-reporting and victim vulnerability are additional problems. Victims may refrain from reporting cybercrimes due to embarrassment, concern about damage to reputation, lack of knowledge about the procedure for reporting, and a perception that justice cannot be obtained. When dealing with financial fraud, rapid flow of money further reduces the opportunity for recovery if there is no quick intervention. It is clear that effective control of cybercrimes involves good reporting systems and coordinated institutional action and not only punishment after the crime has been committed. From the above discussion it is clear that the effectiveness of India's approach lies in the relationship between law, technology, institutions and private players. Cybercrime 2.0 cannot be combated effectively by punishment

alone. A sustainable solution involves flexible laws, technologically efficient institutions, efficient evidence procedures, investigation and protection of rights of individuals. This brings us to the next topic.

6. TOWARDS AN EFFECTIVE LEGAL APPROACH TO CYBERCRIME 2.0

The evolving contours of cybercrime necessitate a shift in the Indian approach to legislation and institutions to an approach which is flexible enough to adapt to technological innovations without infringing upon the fundamental rights of the citizen. It is not about creating a different crime for every new technology. Rather, the approach should be about regulating harmful behaviour and giving the law enough leeway to evolve with changing times. Firstly, the approach taken by Indian cyberlaws must become more neutral to technology and future-proof. In other words, the law needs to be made in terms of intent and behaviour and less dependent upon the technologies themselves. This will allow laws to adapt to changes without the need for constant amending, when a criminal uses some new technology. However, certain areas like AI deception may require special legislation. Moreover, there is a need to enhance special investigations related to cybercrimes. The law enforcement agencies and the investigative agencies must undergo training in terms of digital forensics, digital currency, artificial intelligence, cloud computing, malware and electronic evidence. There should be modern digital forensic laboratories and experts for the cybercrime departments. It will build their institutional capacity at state and district levels so that the complex cybercrimes are not left in the hands of just few specialized agencies. In addition, there is a need to enhance the collection, preservation and authentication of the digital evidence in India. Proper procedure must be followed regarding the preservation of the electronic evidence from the time of identification till its presentation in the court. They must learn about the methods of preserving and obtaining the electronic evidence. They will also have to develop technical capacity to deal with AI generated evidence in the future. It is essential to increase the speed of cooperation among law enforcement, financial institutions and digital platforms in order to provide an adequate response. Investigations into cybercrime often involve information which is in the hands of private companies. Legal means should allow for timely exchange and preservation of such information provided that this request is justified, proportional and documented. In cases of financial crimes, fast communication among the institutions reporting the crime, banks and authorities investigating the situation might increase the chances of freezing or seizing illegally transferred funds. The international nature of cybercrime should be taken more seriously. India needs to increase cooperation with other countries in this matter using all appropriate legal means and investigation techniques. Due to the cross-border nature of cybercrime, its enforcement cannot be limited to the national territory. Equally important should be prevention. Public awareness and digital literacy would decrease the effectiveness of many crimes committed through the use of technology. People should be informed about any suspicious communications, impersonations, phishing scams, fraud and other dangerous activities. They should learn how to report an incident as soon as possible. In addition to that, while enhancing cybersecurity, it is imperative to ensure that certain privacy and due process guarantees are not sacrificed. Increased investigatory powers should not serve as an excuse for the abuse of those powers. Access to digital

information should be lawful, necessary and proportional. Oversight and accountability will preserve people's trust and enable law enforcement to do its job properly. Finally, the Indian model needs to foster constant legal and technological evaluation. The cybersecurity strategy cannot be static because the technologies, platforms and techniques employed by criminals keep on changing. The evaluation process will enable the identification of any new risks posed by technological advancements even before such dangers have caused widespread damage. This approach will enable the law-making process to anticipate any new developments rather than reacting to the damages caused by new technologies. The reform agenda must be to adopt a cybercrime strategy which is flexible, technologically sophisticated and respects rights. Cybercrime 2.0 necessitates increased enforcement of the law, but it must understand that there is no conflict between security and individual freedoms. Such an approach will enable India to effectively tackle cybercrimes in the future.

7. CONCLUSION

Cybercrime is now moving to a new stage where technology, people, and crime are becoming ever more intertwined. Cybercrime 2.0 represents this transition from traditional computer crime to a more flexible and advanced form of cybercriminal activity involving artificial intelligence, synthetic media, social engineering, ransomware, digital finance, and internet-connected devices. In addition to increasing the number of opportunities for offenders, this has increased the potential impact on the victim. India has developed a wide range of legal and institutional frameworks to tackle this problem. The Information Technology Act, 2000 along with the Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023 offer important groundwork for substance offenses, investigation, and electronic evidence. Institutional mechanisms and data governance efforts are also helping to create the cybersecurity framework of India. Yet the efficacy of this legal framework does not depend only on the presence of legal provisions but also on their ability to adapt to changing technological environment. This is primarily because of attribution issues, cross-border investigation, digital evidence, institutional capability, platform collaboration and individual rights. This highlights the need for a different strategy for tackling cybercrime since it cannot be combated using traditional means of criminal law alone. India thus needs an advanced strategy for dealing with cybercrime in the coming future. The strategy should include technology neutral laws, specialized investigation, improved digital forensics capability, international collaboration, raising awareness among the public and proper safeguards on privacy. On the other hand, the effort towards cybersecurity must also be in line with constitutional provisions and due process of law. Overall, Cybercrime 2.0 is not just a technological issue but a legal, institutional and social problem. It will thus depend on how fast India's legal system is able to keep up with the technologies being used by criminals. A strategy that incorporates efficient enforcement and protection of rights can be the basis for this purpose.

Author Contribution

The author conceptualized the research, conducted the literature review and doctrinal analysis, drafted the manuscript, and finalised the article for submission.

Conflict of Interest

Conflict of interest declared none.

Funding

The review presented in the article did not receive any external financial support.

Acknowledgements

The authors would like to acknowledge that no external funding or assistance was received for this research, and therefore, no acknowledgements are necessary.

AI Declaration

The authors declare that no artificial intelligence (AI) tools were used in the preparation, writing, or development of this manuscript.

8. REFERENCES

- Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, Acts of Parliament, 2023 (India).
- Bharatiya Nyaya Sanhita, No. 45 of 2023, Acts of Parliament, 2023 (India).
- Bharatiya Sakshya Adhiniyam, No. 47 of 2023, Acts of Parliament, 2023 (India).
- Government of India, Ministry of Electronics and Information Technology. (2000). *The Information Technology Act, 2000*. Government of India.
- Government of India, Ministry of Electronics and Information Technology. (2022). *National cyber security strategy*. Government of India.
- Government of India, Ministry of Electronics and Information Technology. (2023). *Digital Personal Data Protection Act, 2023*. Government of India.
- Indian Computer Emergency Response Team. (2022). *Guidelines on information security practices for government entities*. Ministry of Electronics and Information Technology, Government of India.
- International Telecommunication Union. (2024). *Global cybersecurity index 2024*. International Telecommunication Union.
- INTERPOL. (2024). *Global cybercrime trend response report*. International Criminal Police Organization.
- Kshetri, N. (2013). Cybercrime and cybersecurity in the digital economy. *Journal of International Commerce, Economics and Policy*, 4(1), 1–24.
- McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence on crime and criminal justice*. Home Office.
- Organisation for Economic Co-operation and Development. (2024). *Digital security and privacy in the digital transformation*. OECD Publishing.
- United Nations Office on Drugs and Crime. (2019). *Comprehensive study on cybercrime*. United Nations.
- Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.
- Yar, M. (2006). *Cybercrime and society*. SAGE Publications.
- World Economic Forum. (2025). *Global cybersecurity outlook 2025*. World Economic Forum.
- World Economic Forum. (2024). *Global risks report 2024*. World Economic Forum.