INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 1 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 1 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-1-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

IMPACT OF CYBER SECURITY LEGISLATIONS IN INDIA ON VARIOUS ASPECTS OF CRIMINAL JUSTICE SCIENCES

AUTHOR - AYUSH AVINASH DAVE, STUDENT AT CHRIST (DEEMED TO BE UNIVERSITY), BENGALURU

BEST CITATION - AYUSH AVINASH DAVE, IMPACT OF CYBER SECURITY LEGISLATIONS IN INDIA ON VARIOUS ASPECTS OF CRIMINAL JUSTICE SCIENCES, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (1) OF 2025, PG. 930-937, APIS – 3920 – 0001 & ISSN - 2583-2344.

AUTHOR

The emergence of the digital era has fundamentally reshaped the very fabric of the society, leading to a paradigm shift in the commission of illicit actions. This transformation includes how people shift and carry out unlawful actions within this technologically enriched milieu. The Information Technology Act (IT), 2000 serves as the cornerstone and provides a legal infrastructure in molding the terrain of criminal investigations and justice with the rise of the digital era. Further, it outlines the violations and provides a sturdy framework for the legal pursuit of cybercrimes. The IT Act is responsible for examining the wide landscape of legal definitions, investigation procedures, data protection and further provides a legal backbone in order to deal with cybercrimes. However, in the dynamic evolution of this legislation to mitigate emerging cyber threats, a simultaneous surfacing of challenge ensues. At the present moment cyber security and criminology lack collaboration which leads to 2 major challenges. Firstly, Cross border cybercrime prosecution presents challenges to international collaboration. Cybersecurity regulations play a crucial role in fostering global partnerships to counter cross-border cyber threats. This is particularly vital in criminal science due to the international nature of cybercrime, by necessitating coordinated efforts in an interconnected world. The second issue involves the ethical aspects of safeguarding data and addressing privacy concerns. This includes balancing cybersecurity imperatives with individual rights, the consequences for victim protection and general ethical issues within the criminal science framework. This paper focuses on providing nuanced study on the growing relationship between cybersecurity laws and criminal sciences by addressing the inherent challenges posed by the transnational scope of cybercrimes while also simultaneously understanding how legal frameworks that protect victims fall short, failing to consistently succeed and how it can be further improved by introducing effective changes and provisions to the law in India.

Keywords: *Data protection, cyber security, IT, investigation.*

Introduction

Cyber security refers to safeguarding data, hardware, software, computers, software resources, communication devices and information from unauthorized use, disclosure, disruption, alteration, or destruction.[1702] It is an essential aspect for individuals as it protects personal information and assets. The swift digitization has ushered in a new age of criminal activity characterized by virtual aspects and global reach. Cybercrime is a broad category of criminal activity that includes financial fraud, data breaches, hacking and online harassment. It is a serious threat to personal safety, national security, and economic stability. With its thriving digital economy and expanding internet-connected population, India is especially vulnerable to these risks. The prevalence of cybercrime and necessity for cybersecurity are becoming significant in socio, political and economic aspects. The term cybercrime is an overarching

[1702] Information Technology Act 2000, s 66.

term including both cyber-enabled and cyber-dependent crimes.[1703] Criminology on the other hand is the scientific examination of the non-legal dimensions of crime and delinquency, covering their origins, correction, and prevention. This field is approached through the perspectives of various disciplines, including anthropology, biology, psychology, psychiatry, economics, and statistics.[1704] As described by Prof Stanton Samenow mindset of criminals and human nature remain constant and do not change[1705]. However, societal changes such as globalization, technology and the internet present new venues and targets for criminals to apply new approaches and innovative methods. As a result, it is critical to comprehend the criminological components of the cybercrime phenomenon in order to gain a better knowledge of essential characteristics of human behavior in cyberspace and many theoretical and empirical methodologies are shared by these domains. Further, The growth of technology has given rise to new difficulties, the most serious of which is the rise in cybercrime. As criminal operations cross national boundaries, enhanced international collaboration in countering cyber threats becomes critical. The interconnected nature of the internet requires a coordinated response from the international community comprising of various nations. Failing which, it will lead to shared threats and linked vulnerabilities as cyber-attacks target the economic stability and leads to risk of national security. Moreover, one of the biggest challenges faced while combating cybercrime is a complex web of cross-border illicit activity. Investigations frequently face jurisdictional issues, preventing law enforcement from pursuing cybercriminals beyond their country borders due to which increased international collaboration is critical to facilitating information sharing, extradition proceedings, and coordinated attempts to overcome these jurisdictional barriers. While cybersecurity measures and international collaborations are critical for combating cybercrime, they must be done with individual data privacy rights in mind. The IT Act aims to strike a balance by including mechanisms for data interception and monitoring that are subject to judicial scrutiny. However, there are still concerns about the possible misuse of these capabilities, as well as the lack of effective controls against data breaches and unauthorized access. Having surmounted these challenges and fostering increased global collaboration, it becomes crucial to delicately navigate the equilibrium between reinforcing security measures and preserving the privacy rights of individuals. Striking this balance necessitates a cooperative endeavor encompassing legal frameworks that not only facilitate international cooperation but also incorporate provisions ensuring the protection of sensitive information and addressing individuals privacy concerns.

History

The Computer Revolution was a major component after Rajiv Gandhi became the prime minister of India in the year 1984. Although there was some initial resistance by 1989, India had more than 1,000 computers[1706] due to reduction in the import taxes and accessories related to it**.** The 1991 Economic Policy also played a major role as the country started experiences an inflow of technology. In the year 1996, the United Nations Commission on International Trade legislation published a model legislation for e-commerce and digital technologies. It also required each country to establish its own rules governing e-commerce and cybercrime. The government of India in order to protect the data of its citizens passed The Information Technology Act, 2000 during the budget session back in the year 2000, criminalizing key cybercrimes such as

[1703] McGuire M., Dowling S. (2013). *Cyber crime: A review of the evidence*. Home Office.
[1704] Hermann Mannheim & Thomas J. Bernard, 'Criminology' (Encyclopedia Britannica) https://www.britannica.com/science/criminology
[1705] Stanton E. Samenow, Inside The Criminal Mind (January 1, 1984 by Crown) 228.
[1706] Samiksha Uniyal, 'How did the Information Technology Act, 2000 come into existence?' (The Cyber Blog India, 4 December 2021) <https://cyberblogindia.in/how-did-the-information-technology-act-2000-come-into-existence/> accessed 5 August 2024

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

hacking[1707] data theft[1708] and online fraud. It also established a legal framework for electronic records[1709] and cyber security procedures. As cybercrime diversified, criminology emerged as a crucial partner in understanding and combating it. Criminologists applied established theories and models like rational choice, social disorganization, and anomie to understand the motivations and the methodology of cybercriminals. But, despite the amendments made to the act in the year 2008[1710] and 2016[1711] challenges persisted. The law enforcement agencies faced challenges dealing with online crime and a fundamental understanding of technology and its involvement in cybercrime is required to adequately analyze and handle these emerging threats.[1712]

Issues

1. Lack of collaboration between cyber crime and criminology

Criminology as defined by Dr Kenny, is the study of socially banned behaviors. This socio-legal study aims to identify the root causes of criminal behavior and propose solutions to reduce crime. It focuses on the legal psychiatric, biological, educational, or socio-legal aspects of criminality. Further, this field of criminal service focuses on the causes, analysis, and prevention of crime. In the present times, cyber criminals have improved their ability to remain anonymous, leading to an increase in Internet-based victimization. Personal information is increasingly being kept on networked computers, putting even casual users at danger. Technological advancements have led to new crime issues that did not exist two decades ago. Cyber criminology has emerged as a unique field within criminology due to the prevalence of illegal acts on the Internet. Cybersecurity research within the realms of computer science and engineering predominantly concentrates on identifying vulnerabilities in both hardware and software. However, there is a notable lack of emphasis on the intentional creation of risks, a phenomenon facilitated by IT companies prioritizing rapid innovation and growth at the expense of security. These risks, manufactured in nature, are adeptly exploited by human adversaries who continually innovate and pose persistent threats. Internet in todays times has been closely linked with national security and military interest. This indicates that online risks are a serious threat to the society and the governmental and defense institutions are required to respond efficiently. Although there is growing interest in cybersecurity across various established fields, the dominance of computer scientists and engineers, with limited contribution from political scientists, is notable. This lack of transdisciplinary involvement seems to have negative implications for both cybersecurity and the understanding of cybercrime.[1713]

2. The lack of international cooperation poses challenges in prosecuting cybercrime across borders.

The ever-increasing use of computers and information communication technologies has created a plethora of new opportunities for crime to occur via electronic methods on a worldwide scale, regardless of national and transnational borders. This has also given rise to transnational cybercrimes. A cybercriminal can perpetrate acts in multiple countries worldwide without the need to leave their own home or cross-national boundaries. The communications can be routed through diverse channels, including local phone companies, long-distance carriers, Internet service providers, wireless and satellite networks. Additionally, the attack may traverse computers located in various countries before targeting

[1707] Information Technology Act 2000, s 66.
[1708] Ibid, s 43.
[1709] Ibid, s 3.
[1710] Information Technology (Amendment) Act 2008.
[1711] Information Technology (Amendment) Act 2016.
[1712] Thomas J. Holt & Danielle C. Graves, 'A Qualitative Analysis of Advance Fee Fraud E-mail Schemes' (2007) 1 *International Journal of Cyber Criminology* 137.

[1713] Benoît Dupont & Chad Whelan, 'Enhancing Relationships between Criminology and Cybersecurity' (2021) 54(1) *Journal of Criminology* 76-92.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 1 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

systems globally. To effectively combat, investigate, and prosecute such crimes, there is a need for international cooperation among countries, law enforcement agencies, and institutions. This collaboration should be supported by laws, international relations, conventions, directives, and recommendations, ultimately leading to the development of a comprehensive set of international guidelines to address cybercrime. However, there are numerous barriers to international cooperation in combating transnational cybercrime. Harmonisation of countries' criminal legislation, the scope of this type of crime, and detecting and identifying criminals across borders. The lack of harmonisation of national legislation causes too many problems.[1714] Countries cannot respond if they do not have a common understanding of the problem. Identifying perpetrators across global borders is essential, as is conducting investigations and securing electronic evidence of their crimes. This ensures that they can be brought to justice in any jurisdiction that complies with fairness and human rights standards. Undertaking this task is inherently challenging.

3. Ethical Considerations in Data Safeguarding and Addressing Privacy Concerns

In a world that is becoming more interconnected with personal and sensitive information which is rapidly flowing through digital channels, the field of cybersecurity plays a crucial role in protecting our data and infrastructure. Yet, in order to shield ourselves against cyber threats, we encounter a significant ethical dilemma which is essentially navigating the delicate equilibrium between upholding individual privacy and guaranteeing collective security. The discourse on the balance between privacy and security stands out to be one of the most significant dilemmas in the domain of cyber security.[1715] This dilemma is around the conflict between maintaining individual privacy and ensuring the collective security of a nation or organisation. In the digital age, where personal information is routinely exchanged and data breaches are a common occurrence, striking the correct balance between these two critical factors has become increasingly difficult. As an essential human right, privacy includes an individual's ability to control their personal information, minimise their exposure to unjustified surveillance, and maintain a sense of autonomy. Data privacy is also concerned with the costs if data privacy is breached, and such costs include the so called hard costs and the soft costs.[1716] Security on the other hand is essential in order to ensure well-being and stability of the society or an organization. This involves the protection of critical infrastructure, preservation of national interests, and the prevention of malicious activities, including cyberattacks and terrorism. Balancing security while respecting individuals' privacy rights is a complex and delicate task.

International Legal Instruments

The Organization for Economic Cooperation and Development (OECD)

The Organisation for Economic Cooperation and Development launched the first comprehensive multinational effort in 1983. It addressed the criminal law issues surrounding computer-related offences. This organisation launched the endeavour to harmonise European cybercrime legislation. In the year 1986, a report was submitted suggesting a list of abuses that government should penalise through criminal law.[1717]

Further in the year 1992, the member countries decided that a minimal list of abuses should be penalised by criminal law to establish a basis for information security in both public and private domains.[1718]This framework includes rules of conduct, legal provisions, and technical

[1714] Javier Lopez & Ahmed Patel, 'International Cooperation to Fight Transnational Cybercrime' (2007).
[1715] Skillfloor, 'The Ethical Dilemmas of Cybersecurity: Balancing Privacy and Security' (Sep 11, 2023).
[1716] Wanbil Lee & Wolfgang Zankl, 'An Ethical Approach to Data Privacy Protection' (2016) ISACA Journal 6.
[1717] Organisation for Economic Co-operation and Development, 'Guidelines for the Security of Information Systems' (Paris, 1992) OCDE/GD(92)190.
[1718] OECD, Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, OECD/LEGAL/0312

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 1 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

measures, with a focus on enforcing baseline security standards for information systems. Nonetheless, these principles require Member States to impose appropriate sanctions, whether legal, administrative, or otherwise, for instances of information system misuse and abuse.

The Council of Europe(CoE): The Cybercrime Convention

The CoE aims to address global concerns about cybercrime, including hacking. The council gave recommendations to the member states to take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime and in particular the guidelines for the national legislatures[1719]. The recommendations for national legislatures consist of a "minimum list," which embodies the collective agreement of the Select Committee of Experts on Computer-Related Crime of the Committee on Crime Problems. This list pertains to specific computer-related abuses that warrant attention under criminal law. Additionally, there is an "optional list," which outlines acts already subjected to penalties in certain states but lacks an international consensus for criminalization.

Several years later, the Council of Europe's Committee of Experts on Crime in Cyber Space prepared a draft to solve the challenges caused by the proliferation of illegal activities on computer networks. It mandated parties to enact legislation addressing cybercrime, guaranteeing that their law enforcement officials possess the requisite procedural powers to investigate and prosecute cybercrime offenses efficiently. Additionally, parties were obligated to extend international cooperation to one another in the collective effort against computer-related crime.[1720]

The G-8 Subgroup on High-Tech Crime

In January 1997, with the backing of the US Government, a Subcommittee on High-tech Crime was established. This working group meets regularly to deliberate on pertinent issues, channelling its efforts towards creating an international network of 24-hour high-tech points of contact to help law enforcement communicate throughout investigations. Professionals can communicate immediately with other professionals in other places to begin all arrangements.[1721] They made recommendations to track terrorist and criminal communications across borders.

In December 1997, they adopted 10 principles and a ten-point action plan to combat high-tech crime.[1722] They firstly wanted to create a comprehensive substantive and procedural cybercrime legislation on an international scale. Other principles included examining legal frameworks to ensure that they foster investigation of high-tech crimes which also ensuring that the legal system is criminalizing offences pertaining to telecommunications. It also considered took into account concerns brought up by high tech crimes when negotiating agreements or arrangements for mutual assistance.

Solutions

1. Lack of collaboration between cybercrime and criminology

The latest Cyber Security Strategy from Australia divides cyberthreats into four categories: Criminals with financial motivations, issue or politically motivated actors, terrorists and extremists, and actors or nation states supported by states.[1723] The first two commonly being an example for cybercrime while the latter being an example for cyber security. The Australian Cyber Security Centre (ACSC)[1724] operates as an independent entity under the

[1719] Council of Europe, Committee of Ministers, Recommendation No. R (89) 9 (Adopted on 13 September 1989 at the 428th meeting of the Ministers' Deputies).
[1720] Convention on Cybercrime, Budapest, 23.XI.2001.
[1721] Jeffrey A. Hart, 'The G8 and the Governance of Cyberspace' (May 2005).
[1722] Meeting of Justice and Interior Ministers of The Eight, Communiqué, Washington, D.C., December 10, 1997.
[1723] Meeting of Justice and Interior Ministers of The Eight, Communiqué, Washington, D.C., December 10, 1997.
[1724] Australian Cyber Security Centre (ACSC), https://www.cyber.gov.au/.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 1 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Australian Signals Directorate (ASD), incorporating personnel from five government agencies specializing in law enforcement, criminal intelligence, security intelligence, signals intelligence, and defence sectors. Its purpose is to establish a hub for sharing private and public sector information, including responding to threats. It is very important to understand that 'crime' and 'security' converge and that is exactly why there is a need for collaboration between cybercrime and criminology. Apart from building an effective body like the ACSC it is also crucial to building international organisations that work together to bridge in this gap. The Five Eyes (FVEY) alliance for example, is a secret society that continuously reshapes geopolitical environments. While most signals intelligence agencies across the Five Eyes are legally prohibited from gathering intelligence within their own borders, many of them have provisions allowing them to support other actors, like national police or security intelligence agencies, upon request. This position also includes giving businesses advice on cybersecurity resilience and doable actions that people may do to increase their level of cyber safety at home.

In India there is a lack of resource constraints wherein, law enforcement agencies lack training and specialized personnel to comeback cybercrime effectively. There should be joint research initiatives between law enforcement agencies and private cybersecurity companies. Furthermore, there should be an effort to converge criminology and cybercrime, ultimately leading to the recognition, prevention, and response to cybercrimes. This interdisciplinary approach should involve the study and understanding of various fields such as criminology, victimology, sociology, information assurance, and computer information systems. By fostering collaboration and integrating insights from these diverse disciplines, we can develop comprehensive strategies to address the complexities of cyber threats effectively.

2. The lack of international cooperation poses challenges in prosecuting cybercrime across borders.

International organisations' initiatives have brought transnational cybercrime to the attention of a global audience and encouraged the harmonisation of legal frameworks across borders. Numerous of these nations are creating regulations, training programmes, and specialised police competencies. In every area of computer-related criminal law reform, international organisations have made a significant contribution to the harmonisation of underlying civil law and criminal laws. But there are several problems in interpreting these cyber crime. The legislators that impose these laws have lack of knowledge in this aspect. They fail to understand the technical problems or if the imposition of a particular act or legislation is even desirable. The very problem relies on the fact that cyber security laws are unclear. The solution to this problem is much more than just awareness and education.

The Organization for Economic Cooperation and Development (OECD) has put forward recommendations for nation states to cooperate across borders at international and domestic levels. They also the national strategies that governments should consider which includes establishment and putting into practice a thorough framework based on current international instruments to help reduce cybercrime.[1725]

Countries need to strengthen international co-operation and mutually assist one another by creating national points of contact to promptly handle inquiries from across borders on digital security risk management. They should essentially work together and promote national digital security risk management so that the risk to other countries does not increase. The stakeholders should also actively participate at

[1725] OECD (2015), Digital Security Risk Management for Economic and Social Prosperity:
OECD Recommendation and Companion Document, OECD Publishing, Paris.
DOI: http://dx.doi.org/10.1787/9789264245471-en.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 1 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

regional and international level in order to exchange information related to digital security risk management. Cross-border investigations and prosecutions could be accelerated by the establishment of specialised courts with judges and law enforcement personnel from many nations. The European Judicial network (EJN)[1726] was established to enhance judicial collaboration between national judges and prosecutors in the fight against international crime. Providing some current background information is one of EJN's responsibilities; this is done, in part, by using a suitable telecommunications network. The jurisdiction of these courts, scope of authority can be agreed upon by treaties amongst different nations. This will give the system a centralized investigation platform and can be effectively used for gathering the evidence which regardless of where it is located, investigators have easy access to vital evidence. Establishing such bodies will provide the convicts consistent law enforcement across various borders.

3. Ethical Considerations in Data Safeguarding and Addressing Privacy Concerns

Striking an optimal balance between security and privacy remains an ongoing challenge. While cybersecurity measures must effectively safeguard data from threats, they should not excessively infringe on individual privacy. Achieving this balance necessitates thoughtful assessment of the unique context and risks, coupled with continuous dialogue and collaboration among stakeholders. The shaping of the digital security landscape heavily relies on cybersecurity policies and legislation, which set forth the guidelines, norms, and rules governing the protection of digital assets and data for individuals, organizations, and governments. These policies are indispensable in preserving the intricate equilibrium between securing sensitive information and guaranteeing the uninterrupted functionality of digital infrastructure.

Before the enactment of the Digital Personal Data Protection (DPDP) Act, 2023[1727] data privacy in India was regulated by a fragmented set of sectoral laws and regulations, leading to confusion and inconsistencies in enforcement. Despite being a notable advancement, the DPDP Act has its limitations. It grants exceptions for government data processing concerning national security objectives.[1728] It omits non-personal data and data processed by the government for national security purposes, thereby leaving a substantial portion of data beyond the scope of the law, potentially exposing it to vulnerabilities and security risks. As per the Act, certain types of sensitive data must be stored in India which could hinder the cross-border data flows. A comprehensive approach is necessary to address the problems with India's data privacy laws and their efficacy in lowering cybersecurity risks.

Data minimization is the practice of just collecting information that is essential for predetermined purposes and discarding information that is no longer needed for those goals. It should be a crucial privacy and cyber risk management practice because it reduces the amount of personal data that an organisation gathers and keeps, which makes it less susceptible to data security incidents and less expensive and time-consuming to protect the data or handle data security incidents. The principle 4 and 5 of the Personal Information Protection and Electronic Document Act specifies limiting collection and limiting use, disclosure and retention of data.[1729]

Furthermore, the broad exemptions that are provided concerns related to national security and the potential misuse of personal data should be rectified by broadening the scope of exceptions. The DPDP Act lacks specific safeguards and in order to prevent the misuse of data the scope of exemption needs to be narrowed down. The DPDP Act, 2023 establishes

[1726] European Judicial Network, 'Judicial Cooperation in Criminal Matters', https://www.ejn-crimjust.europa.eu/ejn2021/Home/EN.

[1727] The Digital Personal Data Protection Act 2023
[1728] Ibid, s 17(2).
[1729] Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5).

the Data Protection Board under Chapter V.[1730] This body is not entirely an independent body as it established by the Central Government and does not have the power to change or introduce legislations. This could lead to biased decision making and limited accountability. There is a dire need of a body that is independent with legislative powers which can issue enforceable rules and guidelines within their jurisdiction. The European Data Protection Board under the General Data Protection Regulation[1731] for example is an independent body with legislative powers which makes it independent from national government and leads to accountability and effective enforcement.

Conclusion

The existing cyber law framework in India, deemed adequate for current requirements, has certain shortcomings. Specifically, the cybersecurity frameworks of certain industry regulators need to be revised to align with the continuous advancements in technology. Recognizing this necessity, Indian authorities are in the process of formulating new policy frameworks to adapt to these evolving changes.

Cybercrime remains a persistent global threat that surpasses national borders, making it a matter of global concern as an organized criminal activity. Various manifestations of cybercrime include online fraud, theft, and cyber terrorism. The efforts to prevent and prosecute computer-related crimes cater to the requirements of all societies, particularly those with developing and still susceptible information technology infrastructures. Enhancing international cooperation necessitates the alignment of substantive laws, a shared set of investigative authorities, and effective and adaptable mutual legal assistance and extradition agreements. Cybercrime should adhere to a worldwide principle of public policy designed to combat and prevent this type of crime by fostering global awareness, improving literacy rates, coordinating legislative initiatives at national, regional, and global levels, and establishing a robust global network of collaboration among national, regional, and international enforcement agencies and police forces.

Cybercrime and traditional crime share some common characteristics, the online environment introduces novel opportunities for both traditional criminals and a distinct category of online wrongdoers. This digital landscape also gives rise to fresh methods and operational possibilities. Although cybersecurity practitioners typically focus on the technological aspects, addressing the "when" and "what" of cybercrimes, there is often insufficient attention given to the "who" the perpetrators are and their motivations. Without a comprehensive understanding of the individuals committing these crimes and their motives, cybersecurity measures remain defensive, reactive, and consistently lag behind the evolving nature of cyber threats.

[1730] The Digital Personal Data Protection Act 2023, s 18.
[1731] European Data Protection Board, 'Art. 68 GDPR' (2018)