Page 2529 - 2544 **DOI:** *https://doij.org/10.10000/IJLMH.117319*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 2

2024

A Critical Analysis of Information Technology Act, 2000 with reference to Cyber Offence and Cyber Security

VISHNU VATSAN MADHUSUDAN[1]

ABSTRACT

The fast spread of modern technology and the advent of the internet has transformed how civilizations work, interact, and do business. This technological evolution, however, has created new concerns, especially in the areas of cybercrime and cybersecurity. This research paper provides an in-depth study of the Information Technology Act 2000, which is a critical legislation in India, having a particular emphasis on its efficacy in combating cybercrime and increasing cybersecurity. The study, based on doctrinal methods, involving mainly secondary sources of data, begins by delving into the terms of cybercrime and cyber-security, as well as their components that include cybercrime categories, consequences, and reasons. It then looks into the Information Technology Act of 2000, the Act's objectives, compliance procedures, and legislative structure intended to combat cyberattacks and secure cyber infrastructure. Furthermore, the study assesses the Information Technology Act's potential to keep up with the ever-changing world of cyber assaults. It evaluates the Act's provisions relating to cyber offences such as computer hacking, data theft, and digital scams, as well as their efficacy in deterring and punishing hackers. The study also explores cybersecurity policies, examining if they are sufficient to preserve important data systems and people' digital confidentiality. Finally, it identifies probable areas for development and legal amendments to better address current cyber dangers and safeguard the best interests of people, institutions, and the country in overall, thus intending to provide input to the continuing cybersecurity issue and assist lawmakers in better protecting the digital realm from potential cyber threats.

***Keywords**: Cybercrime, Cyber-security, Hacking, Information Technology Act, Phishing.*

I. INTRODUCTION

Cybercrime is a newer sort of criminal act in the world. The term "cybercrime" or cyber assault is defined widely as any offence which utilises a computer network in any stage of the crime, and includes critical infrastructure attacks, a scam, online cash laundering, unlawful usage of Internet interactions, identity fraud, the utilisation of technology to expand

[1] Author is a student at School of law, CHRIST (deemed to be university), India.

 [ISSN 2581-5369]

conventional offences, and cyber extortions[2]. Cybercrime is among the most widespread type of offence across contemporary world, and it often has disastrous consequences. Criminals not only wreak tremendous harm to the public and governments, but they also frequently mask their identity. Highly skilled criminals use the internet to commit a range of illegal crimes. In a broader context, cybercrime is any illegal activity in which an electronic device or the internet is utilised as a weapon, an object of attack, or both[3].

ICTs (information and communication technologies) have significantly enhanced the permeable nature of national borders. The Internet's growing accessibility and anonymity combine in a complex relationship that allows unscrupulous and vicious organisations, transnational terrorist organisations, and spy firms to widen their operations abroad[4]. Government-backed[5] internet terrorism in some nations, as well as rogue hackers honing their abilities, have posed new threats to the digital world. The developing connection between criminal syndicates and the global web has consequently exacerbated the digital world's vulnerability[6].

At the same time, new risks to a nation's technological foundation are continually emerging in the domain of national security. The hazards vary from crucial infrastructure safety, cyber criminality, cyber terrorism, digital dangers, and technological warfare to issues with privacy[7].

The Information Technology Act (IT Act) was enacted in the year 2000 and amended in 2008. The updated legislation, from 2008 onwards, emphasises for enhanced safeguarding of data and information privacy through the implementation of established norms against cybercrime. Cyber-crime refers to any kind of violation done with the aim of deliberately damaging the image of a person or organisation through the use of any electronic tool or network, acknowledged by the "Information Technology Act"[8]; yet, the Act does not define “Cybercrime” anywhere, in its provisions[9].

The Information Technology Act of 2000 in India has aimed at integrating legal concepts from multiple such laws related to information technology, adopted previously in many other nations, as well as different regulations dealing with information technology law[10]. The Act grants e-

[2] Nir Kshetri, *Pattern of Global Cyber War and Crime: A Conceptual Framework*, 11(4), Journal of International Management, 541-562.
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] SUSHMA DEVI, *Cyber Security in The National Security Discourse*, Vol. 23, No. 2, World Affairs: The Journal of International Issues, pp. 146-159, 147, 2019.
[8] **KRITI KATHURIA,** *PROVISIONS FOR CYBER CRIMES UNDER IT ACT, 2000*, JOURNAL OF LEGAL RESEARCH AND JUDICIAL SCIENCES, HTTPS://JLRJS.COM/PROVISIONS-FOR-CYBER-CRIMES-UNDER-IT-ACT-2000/
[9] Jatin Patil, *Cyber Laws in India: An Overview*, 4 INDIAN J.L. & LEGAL Rsch. 1 (2022).
[10] Prateek Singh, *Cyber Law in India: IT Act 2000*, Legal Service India E-Law Journal.

 [ISSN 2581-5369]

contracts legal legitimacy and recognises digital signatures. It is a novel type of legislation which renders hacking, data theft, fraud, slander, sexually explicit material, child pornography, and cyber warfare, as criminal offences[11].

(A) Research Problem:

The Information Technology Act, is the primary legislation that regulates cyber security in India. However, there are a number of gaps in knowledge about the Information Technology Act's provisions on cyber offences, out of which, the research presently concentrates on its effectiveness in deterring and punishing cyber criminals and how it can be reconciled with international law on cyber security. The Information Technology Act has been criticized for being too vague and ambiguous in some of its provisions, which has led to uncertainty about how the law should be interpreted and applied. The statute defines a number of cyber offences, including hacking, data theft, cyber bullying, and cyber terrorism. However, the definitions of these offences are often vague and ambiguous, which can make it difficult to determine whether a particular act constitutes a crime.

This uncertainty has made it difficult for law enforcement officials to investigate and prosecute cybercrimes, as they face challenges such as the difficulty of tracing cyber-attacks back to their source, the lack of cooperation from government and the lack of resources dedicated to cybercrime investigations. Hence, rendering the implementation of the statute and its provisions, a difficult task, in order to control and combat the increasing cybercrimes and tighten cyber-security. As technology evolves rapidly, cyber offenses become more sophisticated, thereby necessitating continuous update to the legal framework. The Information Technology Act, being enacted in 2000, therefore, does not include novel measures or means to combat novel cybercrimes, which is another hurdle for the implementation of the provisions of the statute.

(B) Research Objectives

1. To examine the synergy between legal provisions and cybersecurity measures.
2. To analyse how well the Information Technology Act addresses the changing landscape of cyber offenses.
3. To evaluate the challenges faced by law enforcement agencies in effectively enforcing the Information Technology Act against cyber offenders.

https://www.legalserviceindia.com/legal/article-836-cyber-law-in-india-it-act-2000.html

[11] Information Technology Act, 2000, Sec. 66, Sec. 67, No. 21, Acts of Parliament, 2000 (India)

 [ISSN 2581-5369]

4. To examine whether the Act adequately encourages and incentivizes organizations to implement robust cybersecurity practices and incident response plans.

(C) Research Questions

1. What are the fundamental Information Technology Act, 2000 provisions dealing with cybercrime, and how effective is it in curbing cybercrime?
2. What are the gaps in the Information Technology Act, 2000 and what are the challenges faced by India's cyber security infrastructure?
3. What are the amendments to be carried out in Information Technology Act, 2000, to better address the challenges of cybercrime and cyber security?

(D) Research Methodology

The researcher has adopted Doctrinal Method of Research to analyse the Information Technology Act with reference to cyber offence and cyber security in India. The Information Technology Act, 2000 is the primary source which has been referred to and secondary sources which have been referred are law journals, research articles, reference books, newspaper articles and various websites.

II. CYBER CRIME AND CYBER SECURITY

Cybercrime can be described as any action that exploits computer or internet users[12]. A computer linked to a network or an internet connection can be hijacked by fraudsters with malicious intent, causing harm to the user. Cybercrime can be committed by a single individual or a group of organised persons with the purpose of making money or causing a particular loss to internet users by interfering with their gadget. Cybercriminals are organised, use sophisticated strategies, and are extremely technically adept, making it difficult for law enforcement or anyone to spot them.

Cyber security refers to the set of technological advances, methods, and practises that are aimed to secure networks, computers, programmes, and associated information from harm, destruction, or unauthorised access[13]. The method consists of offering security protocols along with safeguards to individuals, processes, and technology that collaborate to assure computer or internet user security and eliminate an array of threats that can impact internet users. Cyber security is primarily provided by technical means available on the internet, legislation enacted

[12] Ally Jaffari Ally & Neha Gadgala, *Addressing Cyber Scam as a Threat to Cyber Security in India*, 5 INT'l J.L. MGMT. & HUMAN. 376 (2022).
[13] *Id.*

 [ISSN 2581-5369]

by a given nation's government, or international pacts between the member nations[14]. Cyber security includes risk and susceptibility diminution, deterrence, international agreement participation, incident response, recovery procedures, resilience and functions such as computer system operations, data protection, and law enforcement. Cyber security approaches, practises, and policies secure digital data stored or utilised on the internet for multiple uses that can be sent or utilised in a database for a particular reason by internet users[15].

Cyber security is essential given that it protects devices attached to the internet that are involved in the facilitating of multiple operations utilised in advancement such as trade, the availability of education for remote education, social media, and also connecting around the globe in which people may communicate to acquire and share their ideas and discover possibilities that exist in various fields which are beneficial for development[16]. This demonstrates how cyber security contributes to the global growth of industries and employment prospects.

There are various cyber – criminal activities that take place, and to tackle such cybercrimes, cyber security becomes extremely essential. Some of these cybercrimes are cyber stalking, hacking, phishing, cyber – squatting, malware, ransomware and trojan attacks, denial of service attacks, identity and data theft, password attacks and many more[17].

III. TYPES OF CYBERCRIMES

1. Tampering of Computer Source Documents

The listing of computer programs, computer instructions, structure, layout, design, and software evaluation of a computer source in any form is referred to as computer source code[18]. Those who purposefully or deliberately cover up, destroy, or modify any computer source code utilised in a computer, computer program, computer infrastructure, or computer network, or who deliberately or consciously induce another to do the same, when the computer source code must be preserved to be maintained by/under law, are regarded as having tampered with the computer source code.

2. Hacking

Hacking is an act of gaining unauthorised control over computer programmes or data. Hacking is committed by anybody who, having an objective of inflicting and understanding that he is most likely to make illicit loss or harm for the general public or any individual, erases, or edits

[14] *Id.*
[15] Prachi Chaudhary, *Cyber Security Threat and Its Laws in India*, 2 LAW Essentials J. 68 (2021).
[16] *Supra* at Note 12
[17] Abhijeet Deb, *Cyber Crime and Judicial Response in India*, 3 INDIAN J.L. & Just. 106 – 117, 107 (2012).
[18] Information Technology Act, 2000, Sec. 65, No. 21, Acts of Parliament, 2000 (India)

 [ISSN 2581-5369]

any data existing in a computer resource, or lowers its worth or utility, or adversely affects it in any way[19].

In broad terms, there are three sorts of hackers: a) the novice group, who are the most recent technological experts and limit their actions to demonstrating their capacity to penetrate systems; b) the "browser" group, who have intermediate technical abilities and obtain unauthorised access to other people's files; c) the cracker group, whose activities vary from duplicating files to causing software and systems to malfunction[20].

3. Cyber Stalking

Cyber stalking entails following an individual's moves throughout the internet and sending alarming and illicit content on social media and other platforms, entering chat groups used by the target, continuously bothering the victim with emails, and so on[21].

4. Cyber Squatting

Cyber-squatting refers to the practise of registering the trade mark, company identity, or brand symbol of another organisation as its own domain title[22], for the goal of keeping it and diverting users to that business domain. Cyber squatters register domain names of popular businesses in the hopes of making quick money, with minor changes, such as the font of a particular alphabet (usually italicizing an alphabet), in the domain name. This misleads the users, trapping them to use the fraudulent website and lose their money. The very first website squatting lawsuit in India was Yahoo.Inc v Akash Arora[23]. In this matter, Yahoo Inc., located in the United States, initiated a restraining complaint over the accused Akash Arora, who had acquired a registered trademark that was confusingly akin to Yahoo Inc. as "Yahoo.com."

5. Phishing

Today's companies can quickly exchange cash for currency kept in computer machines, resulting in computer theft. This organised crime frequently targets credit card holders and private and monetary credit card credentials. It is done by an email that opens with links to websites and directions for entering credit card details, etc. The purpose is to capture confidential data such as credit card numbers, login information, or passwords, or to implant viruses on the machine[24]. Nordea users were bombarded with fraudulent emails carrying

[19] Information Technology Act, 2000, Sec. 66, No. 21, Acts of Parliament, 2000 (India)
[20] *Supra* at note 17
[21] *Supra* at note 17
[22] *Supra* at note 9
[23] Shivani Singh, Cybersquatting in India, IPleaders, https://blog.ipleaders.in/cybersquatting-in-india/
[24] Prachi Chaudhary, *Cyber Security Threat and Its Laws in India*, 2 LAW Essentials J. 68 (2021).

 [ISSN 2581-5369]

malicious software that implanted a keylogger software into their PCs and sent them to a fictitious bank webpage wherein hackers stole login details. This was considered as the biggest online banking scam.

6. Trojan, Malware and Ransomware

Malware or Trojan are nefarious applications such as ransomware, viruses and spyware, that are set up on a system by users by hitting on malicious links[25]. Upon installation, the malware hinders entry to vital network resources, setup further malicious programmes, clandestinely acquire data by sending data from the disc drive (spyware), and impede particular components, rendering the system inoperative[26]. In case of Ransomware, the application demands a 'ransom' in order to be opened, or to function[27]. Kia Motors was forced to hand over to DoppelPaymer, 404 Bitcoins, failing which, hackers blackmailed the organisation with publishing the stolen data, which could bring about a statewide IT and telephone service breakdown.

7. Virus and Worm Attacks

Viruses are algorithms that latch to a system or a file and then disseminate to other computers and documents on the network[28]. They frequently affect the computer's contents by changing or erasing it. Worms, unlike viruses, do not need a host to connect to. They simply produce functional duplicates of themselves and resume this activity till all of the computer's memory space has been encroached upon[29].

8. Cyber Terrorism

Terrorist activity in cyberspace is often characterised as the deliberate deployment of disruptive operations or threats in cyberspace with the purpose to achieve socio-political, ideological and religious, or related agendas. While cybercrime constitutes a local issue, cyberterrorism is a worldwide threat[30].

IV. MOTIVATION FOR CYBERCRIME

A more complete knowledge of cyber-attacks necessitates an investigation of the motivations that drive a hacking unit's behaviour. Because of the character of digital attacks, we can draw parallels from conventional disputes. Warfare on the internet, as in physical reality, occurs for

[25] Abhijeet Deb, *Cyber Crime and Judicial Response in India*, 3 INDIAN J.L. & Just. 106 – 117, 108 (2012).
[26] *Supra* at note 23.
[27] Jatin Patil, *Cyber Laws in India: An Overview*, 4 INDIAN J.L. & LEGAL Rsch. 1 (2022).
[28] *Id.*
[29] *Id.*
[30] Dr. Farooq Ahmad, *Cyber Law in India (Law on Internet)*, 3rd Edn., New Era Law Publications, Delhi, (2008).

 [ISSN 2581-5369]

materialistic as well as intangible purposes such as honour, authority, and reputation[31]. The motivational factors are classified into two types: intrinsic and extrinsic motivation.

The concept of intrinsic motivation proposes that a person's desire for ability and independence is linked to interest and pleasure[32]. Individuals who are genuinely motivated engage in tasks for intrinsic rewards rather than for external rewards. when an individual is intrinsically driven, he or she is inspired to act for reasons of fun or adventure instead of extraneous pushes stresses, or incentives. Maverick hackers, for example, target networks for the sake of a task rather than for monetary gain[33]. Acting on a particular cause is also a type of intrinsic motivation[34]. People can be socialised to act properly and in accordance with a group's values. A normative perspective of action can be triggered by the purpose of acting correctly within the group's standards[35]. A nation, a region, a terrorist organisation, or a collective of hackers could be an organisation to which hackers belong.

Economists also enhanced the knowledge of the manner in which extrinsic forces govern human behaviour, arguing that human behaviour is a function of external incentives[36]. Individual perks may be received immediately or later, but the quantity of monetary incentives and motivation pushing a hacker's behaviour fluctuate in a positive way. Extrinsically driven hackers are consequently more inclined to target networks of organisations with higher levels of economic digitization.

Social norms are another key-factor that supplements the motivation or the reasons for why individuals commit cybercrimes. The prevalence of cyber assaults in a society is proportional to the presence of societal conventions that support such attacks[37]. Cybercrime tends to be warranted in some communities than others. Components of normative organisations may also involve trade groups or industry organisations, which could implement social obligation standards to instil specific behaviours in the hacker group.

Ideology is a significant aspect of cognitive organisations that motivates many hackers' behaviour[38]. A lot of cyber-attacks have been tied to ideological battles. Ideological hackers target websites in order to achieve political goals. While several ideological hackers exhibit

[31] *Supra* at note 2
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] *The Rise of Extremist Hacking and Criminal Syndicates*, http://startechcentral.com/tech/story.asp?file=/2004/10/26/

 [ISSN 2581-5369]

patriotic yearnings, some act in opposition to the country in which they reside. along with country and religion, hackers' objectives are defined by their opposition to globalised capitalism[39]. A clash of ideologies between any organisation and a hacking group, has the potential to end in cyber assaults by the latter organisation over the former. In Indonesia, a crew of hackers targeted the Indonesian police webpage in order to coerce them to release an assailant chief. Attacks by Islamic demonstrators are additional noteworthy instances of ideologically motivated cyber assaults, such as cyber battles between India and Pakistan, and Israel and Palestine.

V. IMPLICATIONS OF CYBER-ATTACKS

Rising cybercrime will likely lead to a greater emphasis on defence and state surveillance in cyberspace[40]. Furthermore, nations will face growing pressure to develop strong deterrent regimes, clear communication and faster national-level reactions to cyber incidents. Government players involved in diplomatic efforts, intelligence, the armed forces, and security agencies will need to collaborate and form a united response to issues. Depending on the form or impact of the cyber assault, states may be compelled to take action with no guarantee of accurate attribution, bringing further concerns about mistrust and war.

Financial damage is one of the most typical impacts of cybercrime on people. Cybercriminals frequently utilise phishing scams, hacking, and malware to get access to a person's financial data, including credit card data, bank accounts, and credentials. This might lead to money being lost due to unauthorised dealings, that may be challenging to recoup[41]. Identity theft is a different serious ramification, where Cybercriminals can exploit stolen private data to register new accounts, obtain loans, and perpetrate other sorts of fraud, causing major legal and administrative difficulties. Cybercrime may trigger psychological distress in along with monetary loss and identity theft[42]. Targets of cybercrime frequently feel abused and in danger, which causes stress and worry. This can have long-term consequences for an individual's psychological well-being.

Organisations can be targeted by cybercriminals in order to obtain intellectual property like proprietary information and patents. Theft of intellectual property may be devastating to firms,

[39] *Supra* at note 36

[40] Jan Neutze, J. Paul Nicholas, *Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms*, Georgetown Journal of International Affairs - International Engagement on Cyber III: State Building on a New Frontier, 3-15, 7, (2013-14) https://www.jstor.org/stable/43134318

[41] Welance, *Impact of Cybercrime on individuals, businesses, and society*. https://www.linkedin.com/pulse/impact-cybercrime-individuals-businesses-society-join-welance

[42] Jaya Vats, Cybercrime : *Types, Consequences, Laws, Protection and Prevention*, IPleaders. https://blog.ipleaders.in/cyber-crime-types-consequences-laws-protection-and-prevention/

especially those that heavily depend on research and development to stay competitive. It may also give rise to reduced income, missed opportunities, and decreasing customer base, potentially influencing the business's future viability[43]. A significant cyberattack may disclose confidential client information, weakening confidence and faith in a company's capacity to safeguard its customers' data. This might result in a loss of loyal clients, a decrease in income, and a decrease in market share.

Cyberbullying and abuse can rise as a result of cybercrime. Cybercriminals may target people or organisations with technology, disseminating damaging material and abusive messages, causing mental and emotional suffering, as well as reputational and social damage. Furthermore, cybercrime has the potential to propagate rumours, which can have major social and political effects.

Social media manipulating is a type of cyberattack in which individuals or organisations are influenced, deceived, or manipulated using social networking platforms for political, economic, or monetary gain[44]. Promoting deceptive data, creating fictitious identities or personalities, and employing automated systems to magnify messages are all examples of this.

VI. INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, officially came into operation in 2000, and governs Indian cyber legislation. The main goal of this Act is to deliver solid legal safeguards for e-commerce through rendering it simple for businesses to register real-time data with government agencies[45]. A variety of alterations were implemented as cyber thieves became more sophisticated, in addition to the human inclination to take advantage of technology.

The Information Technology Act stresses the harsh punishments and fines imposed by the Indian Parliament to safeguard e-governance, e-banking, and e-commerce firms[46]. Its application has been expanded to include all of the modern communication technology. One of the most significant parts of this law is that it has stretched India's territorial borders to include people living outside of India within the purview of this legislation for their criminal acts or omissions, as well as rendering a life sentence mandatory for child pornography[47].

Other elements include the Act providing legal validity to digital documents, electronically signed documents, and the adoption of those information and signatures among the government

[43] Welance, *supra* at note 40.
[44] *Id.*
[45] Jatin Patil, *Cyber Laws in India: An Overview*, 4 INDIAN J.L. & LEGAL Rsch. 1 (2022).
[46] Information Technology Act, 2000, Chapter XI, No. 21, Acts of Parliament, 2000 (India)
[47] Supra at note 23

and its departments for the objective of governance by digital media. Another is the Supervisory Mechanism, which is renamed from Cyber Regulations Appellate Tribunal, to Cyber Appellate Tribunal[48].

If, outside the authorization of the owner or another individual in control of a computer, computer system, or computer network, anyone causes harm to the computer or the entire computer resource, he/she is obliged to pay the damages as recompense to the individual thus affected, under Section 43 of the Act[49]. As stated in Section 43A, a corporate entity that possesses, deals with, or handles any sensitive personal details or data in a computer system that it manages, supervises, or runs is held accountable for compensating to the individual who is impacted, if it is negligent in enforcing and upholding adequate safety practises and techniques.

Anyone unknowingly or deliberately hides, annihilates or modifies any computer source code utilised in any computer resources, or anyone who consciously or willingly allows someone to hide, eliminate, or manipulate any computer source code employed in any computer resources, which is mandated by law to be maintained or managed, shall be imprisoned for up to three years or a monetary penalty of as much as two lakh rupees, or both of them, under Section 65 of the Act. Acts such as transmitting abusive comments via communication services, identity theft, deception by impersonation utilising computer equipment, and breach of confidentiality - all attract a maximum sentence of three years in jail and a fine of one lakh rupees, or both[50].

Whoever, with the goal to endanger India's solidarity, credibility, safety, or sovereignty, or to instil fear in its citizens or any segment of the people, denies or triggers the rejection of accessibility to any person designated to make use of a computer resource; or attempts to break into a computer resource with no authorization; or introduces or leads to the introduction of any computer disruptor, as well as results in or is probable to result in death or injury to persons or crucial infrastructure, is said to have committed cyber-terrorism[51]. Such an individual committing cyber-terrorism is liable for life imprisonment, under Section 66F of the Act.

Pornography is a criminal violation that involves the delivery of explicit material or nudity to a victim without their consent. It is covered by sections 67 and 67A of the IT Act of 2000, as well as sections 292, 293, 294, 500, 506 and 509 of the IPC, and is punishable up to 5 years in prison for first-time offenders, with a fine of 10 lakh rupees[52]. Child pornography is likewise

[48] Information Technology Act, 2000, Sec.48, No. 21, Acts of Parliament, 2000 (India)
[49] *Id*. Sec 43.
[50] *Id*. Sec. 66A – 66E.
[51] *Id*. Sec. 66F.
[52] Devashish Bharuka, *INDIAN INFORMATION TECHNOLOGY ACT, 2000 CRIMINAL PROSECUTION MADE*

encompassed under Section 67B, although it is a more serious infraction because it involves youngsters under the age of 18.

VII. INDIA'S INITIATIVES FOR CYBER SECURITY

The National Cyber Security Policy aims to provide a stable and robust cyberspace for citizens, businesses, and the government at large[53]. Its primary goal is to preserve digital data and infrastructure, while also laying solid groundwork to prevent cyber-attacks by concerted actions of organisations, individuals, processes, and technology. The Office of the Prime Minister established the National Critical Information Infrastructure Protection Centre (NCIIPC) in 2014[54]. It was established in compliance with Section 70 A of the Information Technology Act of 2000.

Following with the government's ambition for a "digital India", the Ministry of Electronics and Information Technology has created the Cyber Surakshit Bharat Initiative to boost India's cybersecurity infrastructure[55]. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) was established[56] to fight and deter online safety infractions. The Computer Emergency Response Team (CERT) recently launched Cyber Swachhta Kendra[57], which is India's cyber security strategy. The Ministry of Home Affairs supervises the Indian Cyber Crime Coordination Centre and, on its suggestion, the Indian Government blacklisted 59 Chinese-origin smartphone apps in June 2020.

The National Cyber-Crime Reporting Portal is an online platform where Indian residents may file reports of cybercrime concerning them[58]. The programme was developed in response to the progress of technology and novel methods, as a result of which the true culprits are coloured once they perform the act, so that the target may report and the investigation team could collaborate on it through the portal.

However, in 2021, the National Crime Records Bureau (NCRB) recorded 52,974 occurrences of cybercrime and in contrast to the prior year, the statistics ascended by approximately 6%[59]. While the facts demonstrate the seriousness of the rising cybercrime rate, it is also concerning

EASY FOR CYBER PSYCHOS, Vol. 44, Journal of the Indian Law Institute, 354-379, 2002.

[53] Prachi Chaudhary, *Cyber Security Threat and Its Laws in India*, 2 LAW Essentials J. 68 (2021).

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Supra* at note 41

[59] *Cyber fraud incidents rising in India: how to file a complaint online on Cyber Crime portal*, February 15, 2023, India Today. https://www.indiatoday.in/technology/features/story/cyber-fraud-incidents-rising-in-india-how-to-file-a-complaint-online-on-cyber-crime-portal-2335149-2023-02-15

 [ISSN 2581-5369]

since the statistics rely solely on reported occurrences. So, if we consider unreported cases, the real number of cybercrime incidences would be significantly higher. This implies the ineffectiveness of the cyber-security measures and the deterrent provisions, under the Information Technology Act, 2000, which subsequently implies the presence of certain gaps in the legislation.

Although the Act has proved to be effective in establishing a framework of legislation in Cyber Domain and addressing a few critical concerns about technological misconduct, it contains a few significant flaws that are still not addressed. The legislation is a toothless law[60], that has been ineffective in imposing punishments or sanctions on abusers who chose to abuse cyberspace's scope. Certain aspects of the legislation require attention.

VIII. GAPS IN THE INFORMATION TECHNOLOGY ACT, 2000

The aforementioned Act claims to apply not just to India as a whole, but additionally to any act or infringement perpetrated by anybody outside of India. Section 1(2) comprises a clause that isn't clearly and positively worded[61]. It is unclear how specific the stated Act will be applicable to any act or infringement perpetrated elsewhere than India by any individual. The IT Act's execution is a major source of worry. Numerous challenges occur in the implementation of the aforementioned Act, as the nature of the Internet has shortened the dimension of the globe, and national boundaries will gradually cease to have a great deal in the digital world.

The Legislation does not address any of the concerns involving domain names[62]. Even domain names weren't defined, and the legislation makes absolutely no mention of the rights and duties of domain name proprietors. It could be maintained that e-commerce relies heavily on the Domain Name System[63], and removing such critical concerns outside the scope of the Act, would make it easier for cybercrimes to take place.

As cyberlaw evolves, so do novel kinds of cybercrime. The IT Act's definitions of crimes are far from exhaustive and makes it seem as if the violations described in the abovementioned Act comprise sole Cyber offences feasible and occurring[64].

The most serious problem regarding this Cyberlaw, is its execution. The Act is silent on how it

[60] Pavan Duggal, *India's IT Act 2000 a toothless tiger?* CSO Online.com. https://www.csoonline.com/article/568061/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html

[61] Pavan Duggal, *Cyberlaw in India: The Information Technology Act 2000 - Some Perspectives*, Mondaq.com. https://www.mondaq.com/india/it-and-internet/13430/cyberlaw-in-india-the-information-technology-act-2000---some-perspectives

[62] *Supra* at note 59

[63] *Supra* at note 60.

[64] *Id.*

will be implemented. Furthermore, with internet usage in India being very high and the governmental and law enforcement officials in general, being computer illiterate, the legislation poses more concerns, than it solves[65].

The Information Technology (Amendment) Act of 2008 doesn't include any provision that assures the user's data is protected while making use of net banking. It is definitely past time for policymakers to take immediate action to safeguard and secure consumers' data, which is managed by many institutions and organisations[66]. The Act, fails to address offences including identity theft. Another gap in the Information Technology Act, 2000 is the dearth of requirements for the establishment of facilities to protect against cyber-attacks from outside sources[67]. The I.T. Act of 2000 must stipulate an apparatus to control cyber-attacks.

Due to these loopholes, the law enforcement authorities face certain challenges, with regard to cybersecurity infrastructure and its maintenance. Cybercrime is getting more advanced, and law enforcement authorities must have the necessary technology to look into and pursue these types of offences. This necessitates significant investments in education and resources.

The Information Technology Act is an emerging law that is still being developed to ensure it keeps pace with the dynamic nature of cybercrime. This renders it harder for authorities to adequately comprehend and implement the law. Law enforcement organisations have particular barriers in executing the Act against various types of cybercrime. For example, investigating and prosecuting crimes involving "anonymous" or encrypted communications are challenging[68]. Furthermore, law enforcement authorities would require help from foreign allies in examining and punishing cyber offences involving servers or other equipment situated abroad[69]. In worst-case scenarios, the authorities' systems become subject to cyber-attacks.

IX. SOLUTIONS

One of the most important components of combating cybercrime is educating the public at large, which can be accomplished by outreach initiatives and campaigns in educational institutions and workplaces. Although technology is readily accessible to the common public, lack of awareness is harmful. This can be a solution to recognize and combat cybercrimes at the very

[65] *Id.*
[66] Gaurav Saluja, *Critical Assessment of Information Technology Act, 2000*, Legal Services India E-Journal. https://www.legalserviceindia.com/legal/article-11163-critical-assessment-of-information-technology-act-2000.html
[67] *Id.*
[68] Soumik Chakraborty and Sreedhar Kusuman, *Critical Appraisal of Information Technology Act*, Academike, (2014) https://www.lawctopus.com/academike/critical-appraisal-information-technology-act-2000/
[69] Diksha Dutt, *An analysis of loopholes under Cyber Law*, LawColumn. https://www.lawcolumn.in/an-analysis-of-loopholes-under-cyber-law/

basic stages, at the societal level.

In the individual level, maintaining the operating system of the device up to date, prevents hackers from abusing software vulnerabilities that could normally facilitate their ability to gain control to your machine and hack it for nefarious reasons. To lessen the effect of data theft, banking and credit card bills ought to be verified on regular intervals, and such credentials shouldn't be kept on the system in order to minimise exploitation. A gadget should be secured by antivirus software for essential internet security because the application serves safeguard against online hazards. As a result of this, such programmes are required for online safety. It also comprises firewall application that safeguards the system from malware, Trojan horses, and other malicious programmes.

Many developing varieties of cybercrime, including data theft, attacks using ransomware, and cryptocurrency-related offences, are not fully covered by the Information Technology Act. The Act must be improved to include these along with other emerging types of cybercrime. The Act also fails to grant police authorities enough authority to examine and punish cybercrime. The Act needs to be revised to reinforce these authorities and allow authorities to keep up with the ever-evolving nature of cybercrime. Because it does not effectively safeguard the confidentiality of victims of cybercrime, the law has to be amended to guarantee that victims' confidentiality is respected throughout every point during the inquiry and trial procedures.

Under the IT Act, the punishments for cybercriminals are comparatively negligible. The Act must be amended to strengthen the sanctions for cybercrime in order to deter offenders and recompense victims who suffered harm, as well as penalise perpetrators to life-long jail instead of the current short prison term. The intermediary entities in the online economy include social networking sites and internet service providers. Nevertheless, the Information Technology Act does not specifically outline intermediaries' rights and obligations in countering cybercrime. The Act should be revised to clarify the responsibility of intermediaries in determining, notifying, and deterring cybercrime.

Ultimately, cybercrime is a worldwide issue that calls for global collaboration to properly address the problem. The Information Technology Act should be amended to allow for greater global interaction in enquiry into cybercrime and punishment.

The Indian government has presently enacted an updated digital data law named as the Digital Personal Data Protection Act, 2023. A number of the deficiencies of the Information Technology Act are intended to be addressed by this new law. Nevertheless, it is critical that the recently enacted law is both extensive and successful in addressing cybercrime. To

 [ISSN 2581-5369]

guarantee that the novel legislation corresponds to the current requirements of the country, the governing body ought to discuss with each stakeholder, namely business leaders, organisations representing civil society, and academia.

X. Conclusion

Technology is a two-sided coin; it offers benefits, but also has adverse repercussions. There are some cases where the utilisation of it is not regarded as an offence, but if it is used by someone who intends to fraudulently utilise it, it falls under cybercrime and constitutes an infraction. Every person must ensure that technology is utilised in a healthy manner.

India happens to be one among the few nations worldwide that has legislations that expressly addresses information technology problems and crimes. A crime-free environment is always ideal and pleasant to hear, but it is merely a wishful thinking. There are numerous statutes in place to prohibit or reduce the prevalence of criminal activity, which is a continuing effort to make the world more secure for the future. The introduction of information technology regulations and Act has opened the ground for combating cybercrime to a certain extent achievable. As a society that is fully reliant on technological advances, cybercrime will continue to surge in the years to come, and lawmakers need to go above and beyond to maintain them at bay.

*****

 [ISSN 2581-5369]