The Infinite
An International Peer Reviewed / Refereed Journal of Multidisciplinary Research

An Online Peer Reviewed / Refereed Journal
Volume 2 | Issue 6 | June 2025
ISSN: 3048-9539 (Online)
Website: www.theinfinite.in

A Study on the New Concern Regarding Cyber Crime

Dr. Kamal Singh Dhakad

Assistant Professor

School of Law and Legal Studies

Sanskriti University, Mathura, U.P.

ARTICLE DETAILS

Research Paper

Keywords :

Cyber-crime, Cyber law, Cyberspace, Digitalization, cyber stalking, cyber terrorism, cyber vandalism, cyber bullying etc.

ABSTRACT

Today in this era we are moving towards a digitization which includes networking as well. This surely offers many advantages in several domains, such as E commerce, communication, freedom of speech and so on. As we are moving forwards in this digital world, many cyber crimes are also increasing wirh the increase of application of this digitization. To prevent and regulate these virtual crimes, there shall be a need to focus on various laws and regulations. There are various laws and measures in India to prevent these crimes examples of laws include the Information Technology Act, 2000, The National Cyber Security Policy and the Digital Personal Data Protection Act (DPDPA). Though the phrase cyber crime lacks an origin or legal reference point; activities like cyber stalking, cyber terrorism, cyber vandalism and cyber bullying are not classified and have no legal footing under cyber crime. This paper emphasizes mainly by highlighting the challenges there, this study underline the urgent need for change in India's cyber legal framework and the several domains where cyber law enforcement under cyber space falls short.

Introduction

In the context of technological progress, about the world is expanding rather positively all around. But with that some anti things also rises to the surface. Rapid expansion of digital and network technology one of these facets helped to create a virtual world of cyberspace. IT laws address every legal issues

connected to online criminality. The necessity for relevant laws and their application has also gained tremendous force as the number of cybercrimes—such as unauthorized access and hacking , Trojan attacks , viruses and worms attacks , denial of services attacks , etc is rising .Cybercrime lacks the source or legal reference . Nortan falsely asserts that cyber-attacks target Indian assets more frequently than they do government and commercial infrastructure. The NCSP has not even begun to address all of the specifies of the cyber threats by any means. This necessitates increased legislative focus, as the offence in this field is expected to rise steadily.

Literature review

As technology keeps getting better, cybercrime have become increasingly more complicated . While the Information Technology Act, 2000 is the main piece of cyber law in India, it is still not strong enough to deal with modern risks like ransom ware, fraud powered by AI and deep fake technology. According to Pavan Duggal's article "Cyber law: The Indian Perspective" (2023), the IT act is reactive instead of proactive, which means it can't predict and stop new types of cybercrime. So in order for regulation and enforcement to work well, law changes must keep up with changes in technology. This is like using fishing net to try to catch lightning. The tools aren't made for the job.

Being able to use and trust digital proof is one of the biggest problems with prosecuting cybercrime. In contrast to regular crime scenes, cyber incidents often involve data that is encrypted,changes quickly, or is kept remotely. In the case of Anvar P.V. vs P.K. Basheer(2014) 10 SCC 473, the Supreme Court said that section 65B of the Indian Evidence Act, 1872 had to be strictly followed in order for computer records to be allowed in court. This perspective was confirmed by the Supreme Court in Arjun Panditrao Khotkar vs Kailash Kushanrao gorantyal (2020) 7 SCC 1, where it stressed the importance of proper certification.

Nandan Kamath in his 2023 book Cyber law and E-Commerce, says that judges need to learn more about technology in order to correctly understand and evaluate electronic evidence. It's like giving someone a map when they are lost in a digital maze- they need to learn how to read the signs.

Legislative Gaps and New Plans for change : Even though the IT (Amendment) Act, 2008 made more online crime punishable, Indian laws still dosen't define the word cybercrime. Introducing the Digital Personal Data security act, 2023 is a big step towards making India's laws more in line with international standard for data security.

Rohas Nagpal in his book "Foundation of Cyber security and Cyber Law," stresses the importance of having a specific Cybercrime Code that covers all the different types of digital crimes and how they change

over time. This is like using a dictionary without looking up a key word- you knows it's important, but you not sure what it means.

Mismatch between past court decisions: Inconsistent court decisions make it even harder to figure it how to apply internet law. In the case of Amit Jaju *v.* State of Maharashtra (2023), the Bombay High Court pointed out that the lack of cyber forensic facilities and specialized courts were major problems that made it hard to get convictions.

Solove and Schwartz in their book Information Privacy law (7th edition, 2023) stated that clear doctrine and skilled judges are needed to protect privacy rights and punish cybercriminals effectively. It's like trying to make a house without a plan; the end result will be different, and it might not be stable.

Jurisdictional constraints in cybercrime investigation: Cybercrime happens all over the world, which makes it hard to decide who is responsible for what. The IT act, 2000 doesn't say much about cross border enforcement, which is why police often don't go after cases that happen outside of their own country. The Karnataka High Court looked into the extraterritorial reach of Indian cyber rules in the case of Karnataka vs Amazon Seller Services Pvt. Ltd (2023), which showed important gaps.

Sood and Suri in their 2023 book named "Data Privacy and Cyber security Laws in India" argue that interest should have clear legal rules that define who has control over what.

Lack of institutions and infrastructure: A strong legal system is not enough by itself; it needs to be paired with strong institutions. Cyber law enforcement is greatly weakened by the lack of cyber forensic labs, trained pros, and ways to settle digital disputes.

Usha Ramanathan in her 2022 book "Law and the Information Society in India" says that for cyber law to be effectively put into action, the government need to be ready and its people need to be trained. To deal with the cybercrime the Supreme Court has said many times that it is important to improve the skills of investigators and judges. (Laws without facilities are like cars without gas: they don't move or work)

Digital Government and National Cyber Security: When it comes to national and e-governance frameworks, cyber security needs a combined method that includes both legal technical safeguards. Between 2018 and 2023, 373 government websites were hacked, as shown in the draft National Cyber Security Strategy (2021) and the 2024 Parliamentary Committee Report on Digital Payments and Online Security

M Sridhar Acharyulu in his 2023 book "Right to Privacy in Digital India," warns that people's rights will stay at risk if privacy laws and cyber security measures don't change together.

Challenges

Cyber security Risks: Cyber dangers like ransom ware, phishing scams, Dos attacks and advanced persistent threats (APTs) are becoming more common, which is threat for national security. Hackers who go after key infrastructure are often helped by organized crime groups or countries.

Weakness in Cloud Computing: Moving storage and activities to the cloud makes people worry about security branches, identity theft and unauthorized access. Cloud setups that aren't right and lack of encryption can make it harder to follow the law.

Use of social media: Because of the internet's anonymity, thieves are more likely to do bad things and are harder to catch and punish. Social media sites are becoming place where fake news, cyber bullying, hate speech, deep fakes and other online illegal activities like terrorism and human trafficking are shared.

Bad use of dark web and cyber crypto currencies: The dark web is where illegal things like selling drugs, arms and human happen. Crypto currencies are used to hide money, pay ransom ware and give financial support to terrorist groups.

Vulnerability and victim's apathy: Victim of cybercrime don't report because they are afraid, embarrassed or don't trust in law enforcement agencies. One more reason is the lack of awareness which makes peoples and small businesses easy target.

Not having appropriate legislation and having impediments to the jurisdiction: Due to the fact that cybercrimes occur in multiple countries, it is difficult to prosecute them.

Insufficient awareness within law enforcement agencies: The technological know-how and tools necessary to investigate and prosecute cybercrimes that are difficult to comprehend are not available to regular police departments.

Misuse AI and deep fake Technology: AI is being used more and more to make deep fakes and fake materials, as well as to spy, phishing and send spam automatically.

Cyber Laws

In the 20th century, new requirements and crimes were added to the law dictionary. It is crucial to have a legal measures in place that provide peace of mind, assist law enforcement and deter thieves, as it is essential to recognize that computers are merely machines and, therefore, not capable of committing

crimes. Because the UNICTRAL knew it had to something about cyber violation. Following that, the General Assembly of the United Nations stated that all states ought to give the State model law serious consideration that they should give it. As part of its duty, the Government of India also agreed that laws needed to be made and has now passes the Information Technology Act, 2000. It got stronger with the additions to it. Before the IT Act, 2000 was made law; all proof in court was in the form of paper documents. It wasn't until after the IT Act was made law that computer record and documents were accepted. Legal recognition of electronic documents is the main things that the act covers. Digital signature can be easily identified. The IT act, 2000 tries to update old laws and gives people ways to deal with the cybercrime. From the point of view of E-commerce in India, the IT Act, 2000 has many good points, such as letting companies use the legal infrastructure for verifying the source and authenticity of electronic communication through digital signature. But it is thought to be the unclear rule in the area of authority when it comes to the internet. Since sec 1(2) says that the act covers all of India, unless the act says otherwise, it also covers any crime or violation of the act that performed outside of India by anyone. It looks like these kinds of rules goes against the idea of fairness. In fact, the word cybercrime at any time even after the IT amendment act, 2008 was passed. The internet rules need to be enforced.

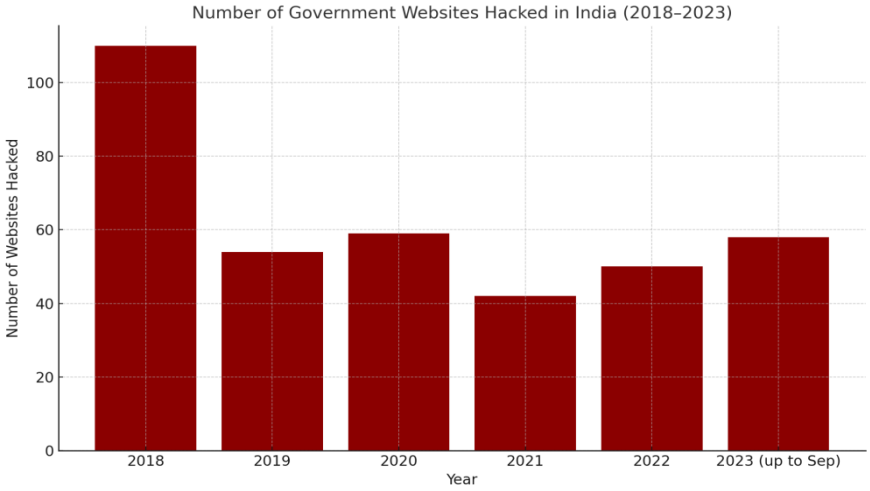
Issues connected to cyber laws

Control over land: Section 46, 48 57 and 61 of the IT act, 2000 talk about how to handle cases and appeals. However these sections do not do a good job of explaining territorial jurisdiction. It can be hard to figure out which police station will look into cybercrime.

Technological concern: The solutions implemented have not effectively addressed the problems and risk associated with cloud computing including the danger of unauthorized access. Big data is a popular new technology, but it raises privacy and security issues. Online scams cost Rs 10,319 crore between April 2021 and December 2023. According to data from the Indian cybercrime coordination centre (14C) provided by CEO Rajesh Kumar, Delhi had the most cybercrime complaint in the country in 2023, with 755 cases per 100,000 inhabitants.

Current statistics of Government website hacks from 2018–2023: The most recent statistics from India's Ministry of Electronics and Information Technology indicate that 373 official governments websites were compromised from 2018-2023. This data was submitted in February 2024 in a report called "Digital Payment and Online Security Measures for data protection" to the Parliamentary Standing

committee on Communication and Information Technology. The rates of government website compromised are as follows



Prospective Outlook

Following the examination of these issues and ideologies, one can anticipate the future implementation of stringent laws addressing such crimes. The enhancement of punitive measures, the introduction of laws tailored to specific problems, and the establishment of non-bailable offences for the majority of perpetrators may contribute to a reduction in cybercrime, allowing the age of technological advancement and digitalization to be devoid of malevolence.

Conclusion

Cybercrime poses a threat to all aspect of life due to its ease of committing and difficult detection. Therefore, it is crucial to strengthen cyber law enforcement efforts. India's legal system is detailed and well-defined, yet laws were based on the political, social, economic and cultural context at the time. At the time, it was difficult to imagine the internet. Despite our master draftsman's expertise the need of cyberspace cannot be anticipated. The internet introduced new legal challenges, prompting the adoption of cyber laws to address these concerns. The internet requires legal infrastructure, as existing laws are insufficient. These considerations highlight the importance of implementing cyber legislation in India.

Reference

- Chaturvedi, M. M., Gupta, M. P., & Bhattacharya, J. (n.d.). A study of India's cyber security infrastructure

- Dalei, P. & Brahme, T. (2014). Cyber legislation and cyber crime in India: A study 2(4), International Journal of Humanities and Applied Science
- Gupta, R. K. (2013). A comparison of cyber legislation against cybercrimes: Indian viewpoint
- IDSA Task Report. March 2012. The cyber security issues of India
- Purohit, A. K. (2011). International Journal of Computer Technology Application, vol. 2, no. 5.
- Singh, T. (n.d.). “Cyber law and IT”
- Taneja, M., & Tiwari, D. B. (2010). “Cyber law”, International Referred Research Journal, 11(21)