

The Legal Framework of Cybercrime in India: Challenges & Solutions

Dr. Sarita Chandel

Bhaskar Law College, Hyderabad

Abstract—The IT Act, 2000 and other provisions of the Indian Penal Code, 1860 constitute the legal framework for combating cyber crimes in India. However, several limitations, including obsolete laws, no or inadequate training of law enforcement officers and cross-border nature of cyber crime, create challenges for effective implementation of these laws. The laws relating to cyber crimes and other conventional laws, if implemented in letter and spirit, can address the challenges relating to cyber crimes. However, it requires training of law enforcement officers, and establishment of Cyber Crime Units, among others. The challenges faced by various countries in combating cyber crimes can be addressed through international cooperation and capacity building.

Index Terms—Legal, Cybercrime, Information, Cybersecurity, enforcement

I. INTRODUCTION

In the last few years, online work and social interaction have taken off in India. The Internet has become our marketplace and principal means of communication. Almost all Indians use the Internet and see it as a positive development. The negative side of this phenomenon has been the exponential increase in cybercrime. Fraud and anonymous harassment have become pervasive.

According to Hindustan Times, in 2024, the first three quarters of the year saw online frauds and scams worth 11,000 crores of rupees (approximately USD 1,300 million).

Harassment and extortion by cybercriminals of all ages has become rampant. Many cybercriminals are beyond the reach of national law enforcement. Phishing, vishing and other social engineering techniques have become prevalent.

The image is a black and white photocopy of a Hindustan Times article. The article describes the increase of cybercrimes for the year 2024. The photocopy includes a portion of the second paragraph

of the article. This paragraph describes and provides a rupee estimate for the first three quarters of 2024 cybercrime reports.

India has several legal inconsistencies concerning cyber crimes. Most of the relevant laws are found in the Information Technology Act of 2000 and in the recommendations of the B.N. Srikrishna Committee. Recommendations address preventing cyber crimes and providing victims' rights. It is generally understood that fully combating cyber crimes requires a multifaceted approach. Creating laws is only one aspect. Law enforcement personnel must be trained about cyber crimes and related laws. In India, this is largely needed at the lower and middle ranks of the police. Simultaneously, the general public must be educated concerning their rights and how to file a complaint.

In your opinion, what is the most effective approach to preventing cyber crimes?

II. CHALLENGES FACED BY OTHER COUNTRIES

Cybercrime is a transnational crime. It requires a multinational approach. Here the challenges posed by cybercrime to a few countries (for example- the US, UK, etc.) will be analyzed. Countries mentioned above have a well-developed and sophisticated legal system. Of late, they have fallen prey to malicious cyber activities like Ransomware. In cases like Germany, cybercrimes of interest are more in the domain of commercial/corporate espionage. In countries like China, most malicious cyber activities are state-sponsored. With the rapid economic growth and increasing commercial transactions of countries like India and Brazil, the financial transactions in the cyberspace have also increased. This situation has attracted transnational criminal activities in the cyberspace. The best approach to combat cyber crimes

in such situations is by forging international and regional partnerships and cooperation.

III. THE LEGAL FRAMEWORK OF CYBER LAWS, INDIA

In order to protect interests of citizens in the cyber space and to achieve other goals of the state, certain laws have been enacted by the Indian Legislature. These laws include, but are not restricted to, the Information Technology Act, 2000.

(1). The Information Technology Act (2000)

Creates a legal channel for conducting businesses and other activities in the field of electronic commerce and transactions in India. The Act also creates a legal framework to combat crimes in the field of information technology and for other related offenses. The Act establishes crimes and prescribes their respective punishment for unauthorized activities in cyberspace, including unauthorized transfer of computer programs and other computer data and cyber terrorism.

The Information Technology Act, 2000 consists of 94 provisions and is classified into one chapter. The Act was enacted on 17th October, 2000 and came into force on the same day. The Act defines different terms used in the Act in section two. The chapter gives overview of different forms of Cyber Crimes under this Act.

The provisions of the Information Technology Act, 2000 govern Despatch of Records, Attribution and Acknowledgment, Secure Records and Digital Signature, Electronic Governance, Intermediary Liability, Offenses, Adjudication, etc. The Act incorporates provisions regarding Electronic Contracts and Electronic Privacy.

(2) The Bharatiya Nyaya Sanhita (BNS), 2023

Some other general provisions of the BNS, 2023 incorporate digital and electronic means for the commission of offenses. The BNS, 2023 creates offenses of sexual harassment, stalking and voyeurism through digital and electronic means.

1. Examples of cyber offenses include but are not limited to, (i) Insult to the Modesty of Women (ii) Offenses Related to Organized Crime (iii) Prejudicial to Sovereignty and Integrity of India (iv) Promoting Enmity between Different groups (v) Other (vi)

Abetment by a Public Servant (vii) Absconding (viii) Omission to Produce Documents (ix) Giving False Evidence (x) Offenses Relating to Public Peace (xi) Offenses Relating to Obscene Acts (xii) Offenses Relating to Defamation.

(3). The Bhartiya Nagarik Suraksha Sanhita, 2023 (BNSS)

The BNSS, inter alia, incorporates definitions of: (a) Process of Reporting and Recording of Cases (b) Conduct of Inquiry and Collection of Evidence (c) Search and Seizure (d) Forensic Science and Admissibility of Evidence.

(4). The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

These Rules stipulate that intermediaries must amend their terms of service and privacy policies to comply with the Rules and also remove unlawful content from their platforms.

Cybercrimes

1. Phishing: The act of tricking a person to provide sensitive information to an impersonated, trustworthy person/entity.
2. Identity Theft: The process of using sensitive information to represent, or impersonate, an individual to conduct transactions in the person's name.
3. Cyber Stalking: Harassing or bullying an individual online or through other electronic means, typically over a period of time.
4. Malware: The intentional transmission of computer software to invasive, damaging, or otherwise compromising a computer system.
5. Online Financial Fraud: Deceiving individuals to Make online, or electronic fund transfers, or other payments, through the medium of false or fraudulent representations.
6. Cyber Terrorism: Terrorist activities or other unlawful acts, intended to coerce a governmental authority, involving the use of computer systems or networks.
7. Cryptojacking: Utilizing another person's computing device to mine Cryptocurrency.

It is important to balance efforts to address cybercrime with other transnational crimes and threats, such as

cyber terrorism. To address the challenges of cyber crime and other transnational crimes, some countries enter into agreements and alliances. International Laws and regulations may govern such alliances and agreements.

IV. TECHNOLOGY

Although the growth of technology has been exponential, limitations still exist especially in the field of Cyber law. The unrestricted nature of the Internet makes it particularly difficult to control cyber crime.

PUBLIC AWARENESS AND EDUCATION

As with other forms of crime, Cyber crime can be prevented with greater public awareness. The public has to be educated on the various methods of online crime.

PRIVACY

Other legal and legitimate rights, interests and freedoms of the individuals may be compromised.

V. LEGAL AND LAW ENFORCEMENT

There are very few, if any, law enforcement and legal professionals trained to address Cyber crimes. Decisions concerning cyber offenses remain rare. On the other hand, there are numerous decisions on traditional offenses, including terrorism, which is committed in the cyber realm.

1. Avnish Bajaj v. State (NCT of Delhi) (2008) ISO DLT 769

This case, among other things, examined the legal limits of an Internet Service Provider's (ISP) liability for illegal contents posted on the ISP's service. The case provided valuable guidance to the judiciary with respect to the interpretation of the provisions of the Information Technology Act, 2000 and in particular, Section 79.

2. Shreya Singhal v. Union of India (2015) 5 SCC 1
This is the only case that examined the intersection of the Constitution of India and the legal framework regulating offenses committed in the cyber realm, as well as other offenses committed outside the country and other offenses committed in the territory of India.

In this case, the petitioners successfully showed that the provisions of Section 66A of the Information Technology Act, 2000, were unconstitutional, as they broadly limited the right of citizens to express and communicate their views.

3. Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473

This case examines rules of evidence relating to electronic documents.

The Court observed that in order to be produced as evidence, an electronic document must conform with the provisions of Section 65B of the Evidence Act, 1872.

4. ARJUN PANDITRAO KHOTKAR V. KAILASH KUSHANRAO GORANTIYAL (2020) 7 SCC 1

The Court relied on Anvar P.V., and extended the scope of admissibility of electronic records as evidence.

Electronic records are covered by specific rules under the Act. The court analyzed these rules. The court looked at the rules regarding the certification of electronic records.

5. State V. Mohd. Afzal & Ors. 20203, 2003 VII AD (2003) 107 (Delhi)D LT 385

The case is important to show how a court can allow the use of a record in its electronic format.

The lower court allowed the Central Bureau of Investigation's report in which computer-generated records were stated to be reliable. The court held that if a party intends to doubt the reliability of the records, then that party will have to produce evidence to show how the records were made. The court rejected the contention that the records were made after the offense was committed.

To prove a case where a person uses a computer or a similar electronic device to commit an offense, a variety of electronic records including E-mail records, and cell phone and similar records, are to be examined. Cyberspace has virtually eliminated time and distance. While that may be good for some, for others (like India) it may mean more work to bring up the infrastructure and other facilities to the level of developed countries. With shrinking of the world, each country has the responsibility to create awareness among its citizens on protecting their interests in the Cyberspace. Law enforcement agencies of countries

have the responsibility to prevent and prosecute cyber law offenders.

(1). In India, there are several (govt and NGO) Organizations which are doing tremendous work to create cyber awareness. Films, documents, posters, CDs and training are some of the many resources used for this cause.

(2). Without sufficient digital literacy, common people will remain ignorant about the threats to their security and interests in the Cyberspace. Unfortunately, a large section of the population in several countries is still un-digitally literate and will remain so for a long time due to lack of investment and other related issues. Therefore, investing on cyberspace threats to the citizens will not be fruitful unless the citizens are made digitally literate to some extent.

(3) Understanding Cyber Hygiene: Just like common sense tells us to practice and maintain proper personal hygiene, the same philosophy should be applied to the digital or cyber world. Examples of cyber hygiene practices include the use of long complex passwords, use of two step verification if it is available, keeping software on our devices up to date, installing up to date antivirus software, and keeping our web browsing practices secure, among others.

(4) Cyber Security in the Classroom: The security and safety of the cyberspace should be taught at all levels of the academic schooling. The teaching should include the legal and ethical aspects of the cyberspace. Teaching children and young adults on cyber security is equally as important as teaching children and young adults' other safety and security practices.

(5) Cyber Security at the Workplace: Just like children and young adults, employees should be trained on the importance of safeguarding employer's and client's information. In the same respect, it is the employer's responsibility to implement practices which secure client's information.

(6) Preventive Role of the Police: In order to combat and respond to cyber crimes, the police rely on and develop many public-private partnerships. The police additionally work to inform the public of various cyber crimes.

(7) Prevention of Cyber Crimes: As hacking becomes more sophisticated, security and law enforcement agencies must develop more proactive measures against cyber crimes. AST and similar agencies must implement more effective tools against cyber crimes and not wait to act against cyber criminals after they strike.

A partnership between law enforcement and the public must be developed to fight cyber crimes. The public must learn to recognize different cyber threats just the way children and school personnel are trained to recognize various threats, fires, and other emergencies. The public has the responsibility to be the first line of defence against cyber threats.

VI. CONCLUSION

The international community has the moral obligation to provide adequate measures to protect vulnerable members of the society, particularly children and the aged. Furthermore, they have the responsibility to ensure that cyber spaces under their jurisdiction are safe.

The digital divide means a large portion of the world's population does not have access to the Internet. It is important that we all learn how to identify security threats.

Children and adults need to be taught these skills. Security threats affect all countries and all employees. It is important to educate the public about the extent of the threats.

It is each person's responsibility to protect the security of the systems that he or she controls and the systems that are connected to it.

When the public is taught about threats to cybersecurity, it should be taught about strategies to protect cyber systems. Collaboration between the public and private sectors should be promoted. Educational programs should be offered in formal and informal settings.

Public and private sectors should take a more active and collaborative approach in developing and implementing prevention and protection measures against emerging cyber threats. Innovations in the field of Cybersecurity and related Laws and Policies should be developed and promoted to reinforce national and international legislation.

REFERENCES

- [1] K. K. Sharma, *Cyber Crime and Cyber Security in India*. [S.l.]: Shree Publication & Distributors, 2016.
- [2] N. Kumar, *Cyber Law: A Legal Framework for Internet Users*. [S.l.]: PHI Learning, 2018.
- [3] S. S. Patil, *Cyber Crime: Investigation and Countermeasures*. [S.l.]: Narosa Publishing House, 2020.
- [4] M. Kumar, *Cyber Crime and Digital Forensics: An Overview*. [S.l.]: Cyber Crime Research Institute, 2021.
- [5] R. Chandrasekhar, *Cyber Crime: A Legal Perspective*. [S.l.]: LexisNexis, 2018.
- [6] T. Agarwal, "Cybercrime in India: Legal framework and enforcement challenges," *International Journal of Law Management & Humanities*, vol. 8, no. 3, 2025.
- [7] K. Rani, "Cybercrime and legal responses in the Indian jurisdiction," *Indian Journal of Law*, vol. 1, no. 1, 2023.
- [8] S. Nakkeeran and D. Singh, "Challenges in cybercrime prevention and legal frameworks in India: An analytical study," *Journal of Advances and Scholarly Researches in Allied Education (JASRAE)*, 2024.
- [9] S. Khandelwal and N. Nawa, "Towards a robust cyber legal framework in India: Bridging the gaps," *International Journal of Leading Research Publication (IJLRP)*, 2024.
- [10] Afzal and A. Singh, "Cybercrimes in India: Challenges and legal reforms," *International Journal of Social Science Research (IJSSR)*, 2026.
- [11] A. Wankhede, "Cybercrimes in India: Identifying challenges and crafting solution," *International Journal of Social Science Research (IJSSR)*, 2026.
- [12] F. Joshi, "Cybercrimes and the legal framework of India," *International Journal of Science and Research Archive (IJSRA)*.