JOURNAL OF CYBER COVERNANCE AND INTELLECTUAL PROPERTY

Volume 1 Article 4

Challenges in Cyber Law Enforcement in India: A Legal Analysis

Nidhi Tiwary

Symbiosis International University Hyderabad

Recommended Citation:

Tiwary (2026) "Challenges in Cyber Law Enforcement in India: A Legal Analysis" Journal of Cyber Governance and Intellectual Property, Vol, 1, Article 4. (DOI)

ABSTRACT

The growth of digital technologies and internet connectivity has played a great role in altering the communication, businesses, and governance in contemporary society. Nevertheless, this technological development has also resulted in a significant increase of cybercrime, posing a new challenge to the legal framework and law enforcement agencies. Cyber activities and offences have laws and regulations that are mainly governed by the Information Technology Act, 2000, in India, which offers a legal means of dealing with crimes in cyberspace. Although this kind of legislation is present, its successful application is a complicated issue because of a number of legal, technological, and institutional problems.

This paper discusses the major issues relating to cyber law enforcement in India. The research methodology will be a doctrinal research which will be based on the interpretation of the statutory provisions, judicial cases, scholarly articles and institutional reports. It addresses challenges like jurisdictional challenges, challenges in gathering and maintaining electronic data, incompetence of the enforcement agencies in matters of technology, and the dynamism in cyber threats.

The study concludes that, although India has formulated a legal system that governs cyberspace, there are still a lot of loopholes in the enforcement of cyber laws. Enforcement of cyber law should be enhanced by ensuring better digital forensic tools, more training of the law enforcers and better coordination of regulators. The research study finds that the challenge of legal reforms, institutional capacity building and international collaboration is critical in ensuring that the issue of cyber law enforcement is successful and the establishment of a safe digital environment.

KEYWORDS

Cybercrimes, Digital technology, Cyber laws, Digital Personal Data Act 2023, Information Technology Act, 2000.

INTRODUCTION

The modern society has changed its interaction patterns due to the fast development of information and communication technology, which has changed the manner in which individuals, businesses and governments interact with each other. The internet and extensive usage of the internet, digital platforms and electronic transactions have generated new opportunities for economic growth and connectivity around the world. Connectivity is one of the necessities of the modern world; without the Internet, people cannot be tied all over the world. It has been studied through various polls on connectivity across the world. As it has been observed, it has expanded as a result of internet connectivity, and people have begun to communicate via the internet. Nevertheless, as a result of this growing interconnection, these crimes have also emerged as cybercrimes like hacking, identity theft, online theft, cyberstalking and data breaches. The necessity of efficient cyber law enforcement has never been as strong as it is now, with cybercriminals taking advantage of the technological weaknesses to the fullest. Enforcement of cybersecurity in all aspects has become a very important factor. Cybersecurity has been established as a requirement in all spheres.

Even though some studies have studied the legal framework of cybercrime in India, it has done so focusing on the statutory provisions and policy developments on the Information Technology Act 2000[1].it has not given much consideration on practical challenges faced by law enforcement agencies in enforcing these laws and consequently this research aims at filling this gap by looking at the challenges facing the enforcement of cyber laws within the legal framework in India and the way forward in enhancing this.

RESEARCH PROBLEM

The available sources on cyber law within India are related to the legal framework of the matter of cybercrime and the development of the Information Technology Act 2000. The increasing nature of cyber threats and the relevance of cybersecurity frameworks have been addressed in several ways. Nevertheless, little has been done to explore the practice issues

[1] Indian Evidence Act, § 65B (India) (1872).

involved in the successful enforcement of these laws by the law enforcement agencies, especially concerning constraints, jurisdictional issues and coordination.

Thus, this paper analyses the consequences of new data protection laws like the Digital Personal Data Act 2023[2] on cyber law enforcement, which are not well researched and recognised. Thus, the given research fills this gap by examining the enforcement by recognising the issues with the existing legal framework and specifying the possible reforms to enhance the enforcement of cyber law in India.

RESEARCH QUESTIONS

---

1 - The role of information technology in dealing with cybercrime in the prevailing legislation.

2- What are the impediments to successful cybercrime investigation?

3- What are the main issues encountered by law enforcing bodies in India with regard to enforcing cyber laws?

4- What are the opportunities of the newly introduced laws like digital personal data protection act 2023[3], which can help enhance law enforcement?

OBJECTIVES

1. To review the legal framework of cybercrime.

2. To examine the issues affecting the law enforcement agencies.

3. To assess the weaknesses in cyber law enforcement.

4. To offer reforms that will enhance the cyber law enforcement system.

[2] Digital Personal Data Protection Act, 3 (India) (2023).
[3] National Crime Records Bureau, *Crime in India Report*, https://ncrb.gov.in

LITERATURE REVIEW

Following the rapid expansion of digitalisation, there has been an expansion of the cyber activities in the world with the increasing dependence on the internet to communicate, conduct business, governance and financial transactions, cybercrime has become a major challenge facing the legal systems in different parts of the world. This has led to the emergence of literature in the world. Other issues of cyber law have been explored by scholars, policy makers and legal institutions such as statutory frameworks, judicial interpretations as well as institutional capacity and the dynamic nature of cyber threats.

Most literature available is concerned with the governing cyber activities in India, specifically the Information Technology Act 2000[4] That is the major legislation of cybercrime in the country. The provisions of the act and its role in regulating digital activities have been greatly discussed by legal scholars. Their works underlined the fact that the act gives the status of law to the electronic records and electronic signatures and sets the punishment of various cyber crimes such as hacking, identity theft and other unauthorised entry to computer systems. These publications indicate the significance of the act in establishing a legal system to help in the recognition of cyber offences in India. Nevertheless, a number of scholars suggest that though it is important, the act has some drawbacks, particularly in addressing the fast-changing cyber threats and other emerging technologies.

India's judiciary has contributed significantly to the legal environment of cyber regulation in India. Shreya Singhal vs Union of India[5] is considered to be one of the most famous judicial rulings in this case, as the Supreme Court overturned the section 66A of the Information Technology Act, stating that the section was unconstitutional, as it infringed the basic right to freedom of speech and expression as stipulated by Article 19(1) (a)[6] of the Constitution. The decision has been construed as a major stride in ending the abuse of cyber laws in order to restrict the freedom of expression on the internet. Meanwhile, certain researchers believe that

[4] Information Technology Act, 43, 66 (2000).
[5] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).
[6] Article 19(1) (a), Constitution of India, 1950

such a decision safeguarded the basic rights, yet it also created an issue with the regulatory ability of the state to regulate harmful online material. This debate underscores the debate that exists between regulation and constitutional freedoms that still continue to define the evolution of cyber law in India.

The other court ruling that took place in the area of cyber law is the case in KS Puttaswamy v Union of India, where the Supreme Court of India acknowledged that the right to privacy was a fundamental right under Article 21. The court emphasised the fact that in the era of the digital world, personal information and the privacy of information is to be provided with security, because of the growing use of digital platforms and online services. It established a constitutional basis for increased data protection regulations, such as the Digital Personal Data Protection Act, 2023[7]. On the side of the cyber law enforcers, the case brings out the need to balance efficient cybercrime investigation with the right to privacy as an individual.

Moreover, some studies have examined how regulators and police can deal with cybercrime. The trends and patterns of cybercrime in India are important regarding reports published by the National Crime Records Bureau. Based on these credible reports, the cases of cybercrime reported have grown remarkably within the last ten years. Researchers who study these reports believe that cybercrime is increasing in close connection to the development of digital infrastructure and the increased utilisation of online platforms to conduct money transactions and communication. Nevertheless, these research works have also noted that police departments are usually struggling to investigate cyber crimes because of the technical nature of cybercrime and the unavailability of specialised equipment.

The other significant body of literature is that concerned with institutional and technological issues of enforcement agencies. Problems which have been brought to the forefront by scholars include the absence of sufficient cyber forensic infrastructure, deficiency of skilled workers and challenges in gathering and maintaining on-electronic evidence. The investigation of cybercrimes usually involves a lot of technical skills and investigative equipment that might not be easily accessible by the law enforcement agencies. More so, other reports by agencies like INTERPOL have underscored the fact that efficient cybercrime control must be characterised by high levels of international cooperation, knowledge and power exchange among law enforcement agencies in various jurisdictions.

[7] INTERPOL, *Cybercrime*, https://www.interpol.int/en/Crimes/Cybercrime

The emerging implications of the new data protection frameworks have also started being investigated by recent scholarship in enhancing cybersecurity governance. The Personal Data Protection Act 2023[8] is a developmental move in the area of digital data protection. According to the scholars, the act imposes significant responsibilities on organisations that handle the personal data and puts in place systems to protect the privacy of individuals in the online world. Meanwhile, other researchers have also expressed concern with the application of the act especially in terms of the institutional capacity that is needed to enforce it effectively. The interaction between data protection legislation and the current laws against cybercrime is in the early stages of its development, and researchers still argue about the nature of the interaction between this structure in practice.

Although the knowledge on cyber law and cybersecurity control is increasing, there are some gaps that exist in the current body of literature. The majority of the existing literature focuses on statutory provisions, policy frameworks and theoretical facets of cyber regulation. There has been comparatively minimal focus on practical enforcement issues of law enforcement agencies especially in the Indian context , also the relationship between the emerging legislations on data protection and the available cybercrime enforcement mechanism have not been well addressed.

Thus, the study aims at adding to the already existing literature to research the practical issues related to cyber law enforcement in India. The paper also attempts to make recommendations that can enhance the institutional capability and make cyber law enforcement mechanisms more effective in the increasingly dynamic digital environment.

METHODOLOGY

This research adopts a doctrinal legal research methodology to interpret the challenges associated with cyber law enforcement in India. Doctrinal research involves the systematic analysis of principles, legal rules and frameworks through the examination of statutes, judicial decisions and scholarly writings. The primary objective of this study is to analyse the existing legal framework governing cybercrime and to evaluate the effectiveness of

[8] Digital Personal Data Protection Act, 3 (2023).

enforcement mechanisms. This doctrinal method is considered the most appropriate approach for this research.

This study relies on both primary and secondary legal sources. Primary sources include statutory provisions, judicial precedents and legal framework governing cybercrime and to evaluate the effectiveness of the enforcement mechanism, the doctrinal method is considered the most appropriate approach for this research. The research analyses the provisions of the Information Technology Act 2000[9]It acts as the principal legislation governing cyber activities and cyber offences in India. It addresses offences such as theft, data breaches and online fraud. Additionally the research examines the enacted Digital Personal Data Protection Act 2023[10], which gives a regulatory framework for the protection and processing of digital personal data. The interaction between these two regulations has been analysed to understand how upcoming data protection laws influence cyber law enforcement.

The research relies on secondary sources as well, which include academic books, peer-reviewed journal articles, legal commentaries and policy reports. Reports published by the national crime records bureau are examined to understand the statistical trends and patterns of cybercrime in India. These reports provide insights into the growing incidents of cyber offences and the practical challenges faced by enforcement authorities. It also has a comparative perspective, which examines international approaches to cybercrime regulation and law enforcement. It also seeks to examine the existing arch gap and evaluate the effectiveness of enforcement mechanisms. Altogether, this methodological approach helps in proposing informed legal and policy recommendations aimed at strengthening cyber law enforcement in India.

LAW IN INDIA: LEGAL FRAMEWORK OF CYBER LAW

The fast pace of development of digital technology has led to the need to transform legal systems to respond and control the activities in cyberspace, in addition to recognizing and responding to cyber crimes. In India, the major policy that contains the governing laws of

[9] Nir Kshetri, *Cybercrime and Cybersecurity in India* 88 (Cambridge Univ. Press ed. 2020).
[10] Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act Information*, https://www.meity.gov.in

cyber activities is the Information Technology Act, 2000. This legislation was passed to control transactions on the web and offer protection. It came up with provisions along with offences committed in terms of unauthorised hacking systems, theft of identity, as well as data theft. Some of the sections in this act, which address unauthorised access and damage against computer systems include sections 33 and section 66 of the act.[11]

The act was further revised to add more scope of cyber offence and enhance cybersecurity. The amendment added subtleties that deal with identity theft, online terrorism and online fraud, even after amendment, implementation is left to the investigative agencies and the courts.

Despite the fact that India has set a legal framework in order to control cyberspace, a number of scholars believe that the problem is not the lack of laws, but the inability to enforce and implement the laws effectively.

CYBER LAW ENFORCEMENT AMIDST JURISDICTIONAL PROBLEMS

One of the largest issues on enforcement of cyber laws is the international nature of cyberspace. Cybercrimes are normally committed over digital networks across national borders. As a result, the perpetrator, victim and computerized infrastructure involved in the criminal activity may be located in a wide range of jurisdictions. This presents a great challenge to the criminal justice organisations when probing and prosecuting cyber crimes.[12]

This is illustrated by the fact that someone who is in a given country may have a victim in another country and carry out a cybercrime using the assistance of servers in a third country. This complicates the process of taking legal proceedings as the laws of two or more jurisdictions can be applied simultaneously. The global cyber laws are not harmonised thus making enforcement even more challenging.

Other global agencies such as INTERPOL have also encouraged cross-border cooperation in dealing with cybercrime. Mutual legal assistance treaties and joint investigations are important tools, which should be employed to combat cyber offences. However, many

[11] World Economic Forum, *Global Cybersecurity Outlook 2025*, https://www.weforum.org
[12] Reserve Bank of India, *Report on Trends and Progress of Banking in India*, https://www.rbi.org.in

developing countries are still faced with the challenge of formulating a powerful international cooperation system.

The next important question that has to be addressed by cyber law enforcement is related to the collection of electronic evidence, its preservation, and admissibility. The digital evidence is very volatile and therefore liable to changes, deletion or manipulation as opposed to the traditional evidence. Therefore, the police departments are recommended to comply with strict technical procedures when obtaining digital evidence during the investigation of computer crime.

The criminal investigating officers are supposed to ensure that they acquire electronic evidence in a form that satisfies the legal provisions in order to prevent legal issues in the court of law. However, in many police departments, there is a lack of specialized training and digital forensic tools and resources, which could be a hindrance to successful investigation and prosecution of cyber crimes.[13]

CYBER REGULATIONS, CONSTITUTIONAL AND PRIVACY ISSUES

In K.S. Puttaswamy vs Union of India[14], the Court declared the right to privacy as a fundamental right under Article 21[15] of the Constitution. The Court emphasised the fact that in the digital age, personal information and informational privacy ought to be ensured. The consequences of this ruling on cyber law enforcement are far-reaching since the ruling requires the authorities to balance between investigative and constitutional rights.

The same is also true regarding the ending of the case in the case of Shreya Singhal v. Union of India, which highlighted the necessity to protect the freedom of expression and speech on the Internet. The Supreme Court ruled that section 66A of the Information Technology Act [16]was unlawful as it had violated constitutional freedoms. The ruling was in favour of the notion that basic rights should not be at stake when it comes to cyber regulation.

[13] K. Jaishankar, *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* 101 (CRC Press ed. 2011).
[14] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).
[15] Nir Kshetri, *Cybercrime and Cybersecurity in India* 88 (Cambridge Univ. Press ed. 2020).
[16] Information Technology Act, 43, 66 (2000).

These judicial decisions can be taken as an illustration of the present-day dilemma between the application of cybersecurity and civil liberties. A competent cyber law enforcement should therefore be in a position to operate under a legal system that promotes constitutional values and addresses emerging cyber threats.

TECHNOLOGICAL AND INSTITUTIONAL ISSUES

Cyber law enforcement is also faced with institutional and technological challenges other than legal issues. Cybercrime must also be studied, requiring expert knowledge on digital systems, advanced forensic tools and technical knowledge, too. However, police departments are ill-equipped and trained to cope with complex cybercrime challenges.

Based on the reports published by the National Crime Records Bureau, a slow increase in cases of cybercrime[17] has then been witnessed throughout India. This is because the investigative agencies have not been expanding their capacity as the number of offences grows. This is what leads to a delay in investigation and the effectiveness of enforcing mechanisms.

Therefore, the future of transforming into a more effective enforcer of cyber law should not just be founded on changes of law but also on capacity building, technical education, and improved digital forensic structure.

DISCUSSION

This research paper indicates that the implementation of cyber laws in India has a number of critical issues. Despite the fact that the nation has established a legal framework that is well developed through the enactment of policies such as the Information Technology law 2000 and the Digital Protection Act 2023, putting it into practice is an uphill task due to the legal, institutional and technical challenges.

[17] Aparna Viswanathan, Cyber Law in India: Challenges and Emerging Trends, 10 Indian J. L. & Tech. 45 (2014).

One of the key challenges that has been raised in this paper is the issue of complexity in the jurisdiction of cybercrime. Another important matter is the strengthening of international cooperation through the use of international treaties and cooperation in the circumstances of strengthening cybercrime law enforcement. The second problem is connected with the gathering and admissibility of electronic evidence. Special abilities should also be possessed by the police officers and they should follow the right procedures to collect, store and present digital evidence during an investigation of cybercrime. The shortage of competency and digital forensic infrastructures might be a hitch to successful implementation of cybercrime. The other area that the research addresses is the necessity to find a balance between the enforcement of the cyber laws and protection of constitutional rights. Cases like K.S. Puttaswamy vs Union of India[18], Shreya Singhal vs Union of India. [19]Several reforms can be considered to enhance and empower the cyber law enforcement. Firstly, the law enforcement agencies should be enhanced in terms of the technical training and digital forensic skills to better the functioning of cybercrime investigation. Second, this can be enhanced by the regulation agencies and the investigative agencies to coordinate their work. Third, the government can use high-tech cybersecurity infrastructure to defeat the rising menace of cybercrimes.

In general, this paper demonstrates that the alternatives to cybercrime are multidimensional, and reflect the legal changes, the formation of institutional capacity and international cooperation. This will add to the fact that the cyber laws are not only effectively formulated but also implemented in the digital age by empowering such points.

FINDINGS

This study raises several significant points to the use of the laws of the cyber sphere in India. First of all, India has developed an organised legal framework which is applied to address cyber crimes by enacting laws such as the Information Technology Act 2000. The triumph largely depends on the ability of law-enforcing institutions. The study concludes that the lack

[18] P.S.A. Pillai, *Criminal Law* 450 (14th ed. 2019).
[19] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).

of legal provisions is not the issue of primary concern, but rather practical difficulties in the implementation.[20]

Second, the paper refers to the notion of jurisdictional complexities as one of the notable impediments to effective cyber law enforcement. Cybercrime frequently occurs when an offender, a victim and computer infrastructure are located in different nations. This transnationalism by cybercrime makes it difficult to detect and try cyber criminals, particularly when there is a sluggish or weak response of international collaboration.

The other critical finding relates to the collection and management of electronic evidence in relation to investigations involving cybercrimes. Numerous judicial rulings have shown that electronic evidence must adhere to very tough legal prerequisites to be admissible in court. Whereas any form of evidence requires certain evidentiary standards that should be implemented to ensure the integrity of digital evidence, they also require the investigators to be capable of possessing some technical competencies and various advanced digital forensic tools.[21]

In the paper, the issue of cyber law enforcement is also identified to be limited in scope to constitutional rights. The renowned cases are K S Puttaswamy VS Union of India[22] and Shreya Singhal VS Union of India [23]that focuses on the necessity to safeguard the privacy and the freedom of speech on the internet. These decisions demonstrate that cyber regulation must be moderate between appropriate enforcement of the law, and protection of fundamental rights**.**

Finally, the study shows that the institutional factors, such as the lack of skilled labour force, the lack of digital forensic laboratories, and the lack of technical expertise, affect the ability of law enforcement agencies to effectively combat cybercrime to some extent.

CONCLUSION

The huge expansion of digital technologies has altered modern society and provided a possibility to communicate, economically develop and be in touch everywhere across the

[20] Jonathan Rosenoer, *Cyber Law: The Law of the Internet* 120 (Springer ed. 1997).
[21] Rohas Nagpal, *Cyber Crime and Investigation* 67 (Asia Law House ed. 2018).
[22] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (Supreme Court of India).
[23] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).

globe. However, it is also through this digital revolution that cybercrime has increased tremendously and therefore, effective enforcement of cyber laws has been even greater now. The laws governing cyber practices in India have been formulated over the years, and some of them include the Information Technology Act 2000 and the Digital Personal Data Protection Act 2023 (more recent). These are supposed to tame cyberspace, secure computers, and counter cyber crimes.

Despite the current legal regulations, this research demonstrates that several issues continue to plague the welfare of cyber law enforcement, which the unlimited character of cyberspace brings about issues of jurisdiction, and the collection and preservation of electronic information requires certain technical expertise.[24] Besides, the dynamic nature of technology makes it difficult to stay afloat in the face of the evolving cyber threats to legal systems and enforcement organs. A holistic approach of changing the law, instruction and augmentation of technological facilities should be adopted to improve cyber law enforcement. The police should be furnished with skills in computer investigations and skills in forensic analysis. In addition to this, more intimate mechanisms of global liaison and enhanced coordination among the regulatory units are required to address the transnational nature of cybercrime.

In the conclusion, the author states that though India has been striving hard to establish a legal system that will regulate cyberspace, more still needs to be done to ensure the efficacy of the cyber laws. In order to establish a secure and more stable cyberspace in the future, the strengthening of the enforcement mechanisms will be required, the improvement of technical capabilities and the increase of awareness of the problem concerning cybersecurity.[25]

[24] Justice Yatindra Singh, *Cyber Laws* 210 (Universal Law Publishing ed. 2017).
[25] Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* 154 (Universal Law Publishing ed. 2020).