Journal of Advances and Scholarly Researches in Allied Education
Vol. 21, Issue No. 1, January-2024, ISSN 2230-7540

Challenges in Cybercrime Prevention and Legal Frameworks in India: An Analytical Study

S. Nakkeeran[1]*, Dr. Dharamveer Singh[2]

[1] Research Scholar, University of Technology, Jaipur, Rajasthan, India

Email: advocatekeeran@gmail.com

[2] Associate Professor, Dept.of Law, University of Technology, Jaipur, Rajasthan, India

Abstract - The rise of cybercrime has been a major problem for countries, businesses, and people all around the world. The purpose of this study is to shed light on the difficulties in enforcing laws against cybercrime in India and to highlight the critical need for such a framework in order to stem the tide of this rapidly expanding threat. There has been an upsurge in cybercrime in India in recent years. The fact that it has such a detrimental effect on people's social and economic life makes it a very worrying issue. Data from cybercrime cases prosecuted in India's most susceptible states and cities under the IT Act and the Indian Penal Code formed the basis of our study. In addition, we have examined the data of cybercrime instances perpetrated by individuals of varying ages. In addition to outlining the many reasons for cybercrime and the crimes themselves, this article also provides crucial recommendations on how to reduce cybercrime. Both the investigation and punishment of cybercriminals and the general deterrent against cybercrimes are weakened by these obstacles. To tackle the unique problems posed by cybercrime in India, this study acknowledges the need of a thorough legislative framework and suggests important components that should be included in the laws.

Keywords: Cyber, crime, IT Act, Indian Penal Code, Offences

----------X----------

INTRODUCTION

Any unlawful conduct that involves the use of, or damage to, a computer, computer network, or network-connected device is known as a cybercrime. Almost all cybercrimes are perpetrated by cybercriminals or hackers driven by financial gain. Anyone, from people to corporations, may perpetrate cybercrime. Some cybercriminals use state-of-the-art techniques, are technically adept, and are well organised. There are some hackers that lack experience. Sometimes, the goal of cybercrime is to damage computers for purposes other than stealing their data. These could be personal or related to politics. When criminals commit their crimes using computers or other digital devices, they are committing cybercrime. A computer may play several roles in this kind of crime: victim, perpetrator, or evidence custodian. "Cybercrime" is shorthand for any kind of wrongdoing that occurs in the digital realm. Examples abound, and they include fraud, malware-like infections, cyberstalking, and identity theft. Today, organisations, government agencies, and people must prioritise the control, prevention, and investigation of cyber activities. This is because information technology is the backbone of most information processing. Acquiring and retaining highly competent cybercrime specialists is an issue that neither government nor businesses can afford to ignore. In the past, individuals or small groups were the main perpetrators of cybercrime. Cybercriminal networks that bring together individuals on a global scale to commit infractions are becoming more complex. There is no longer any room for ego or competence as motivating factors for hackers. Instead, they want to cash in on their expertise quickly. In order to generate money with little effort, they are taking use of their skills in sniping, deceiving, and exploiting others. Cybercrime is a major problem now.

LITERATURE REVIEW

Kethineni, S. (2019), Criminal acts perpetrated via the use of computer systems or networks are known as cybercrime. Unfortunately, cybercrime is a global problem. Internet usage and abuse have proliferated nationwide with the country's rapid technical advancements during the last two decades. According to Mallapur (2016), the United States and China are at the top of the worldwide rankings for "malicious activity," while India is third. Additionally, Statista predicts that by 2022, there will be about

512 million Internet users in India, up from over 330 million in 2017. The nation has seen a rise in cybercrimes such phishing, code injection, identity theft, bank fraud, transfer of sexually explicit materials, cyberstalking, and cyberbullying as a result of these developments. This chapter offers a concise overview of the Indian government, including topics such as the branches of law (executive, legislative, and judiciary), cybercrime laws, and the scope and kind of cybercrime. Cybercrime is also discussed in the country's current discourse.

P.B. Ajoy (2022), The incidence of cybercrimes and its negative repercussions have prompted some countries to pass legislation to address the issue. Cybercrime is on the rise, according to the data that is available, even though laws have been passed to combat it. When it comes to cybercrime, the criminal justice system falls short for a number of reasons. Some of these factors include problems with jurisdiction, difficulties with extradition, problems with the law enforcement machinery, difficulties in identifying, locating, and arresting cybercriminals, a lack of experts, problems with technology, problems with international law, and problems with cybercrime data (such as underreporting of cybercrimes). It is necessary to concentrate on cybercrime preventive measures as, as things are, criminal law cannot adequately address cybercrime.

(Misra, A., & Chacko, M., 2021), Hacks, ransomware attacks, and other cybersecurity breaches are more common in India despite the country having one of the world's biggest software personnel infrastructures. Due to the absence of a unified cybersecurity framework, several sectoral legislation and criminal codes interact in an often bewildering way, leading to substantial uncertainty. The purpose of this article is to survey the many statutes, rules, and policies that make up India's cybersecurity framework and to point out problems that stem from this disjointed approach.

Kaur, M., Saini, M. (2023), Cyberbullying on different social media sites is a growing problem in today's technologically advanced world, which puts young people at risk. The alarming numbers of cyberbullying continue to rise year after year, with disastrous results. The Indian government has responded to this online danger by establishing cyber cells, a number of hotlines (particularly for women and children), complaint boxes, and stringent legislative measures to prevent and punish cybercrimes. The efforts that are pertinent are assessed in this study. In addition, a survey is carried out to get a better understanding of cyberbullying on college and university campuses. The survey covers several causes of cyberbullying among young people and offers some solutions to this problem.

In 2016, Umejiaku and Anyaegby The emergence of globalisation provided nations with a chance to choose their economic futures. Supported by computers and allowing for seamless communication, IT quickly became a need, and the advent of the World Wide Web (www) inspired awe at the seemingly endless possibilities, but also the impending perils and hazards. Despite this, online shopping has significant promise for the future. Everything used to be done in writing and sent over the mail before this age, but that all changed when the internet came along. The UN took action on data protection due to the increase of email interactions. In 1996, the UN Commission on International Trade issued a "Model Law" based on that rationale. Basically, according to Samuel Huntington, the globe has become a "flat world" and a "global village" because to IT. The economic, commercial, social, and educational facets of society have all benefited.

PREVENTIVE MEASURES TO HANDLE CYBER CRIME

Despite of the cyber laws and government policies, we can take several measures to avoid cybercrime in our society. The followings [7] are few suggestions:

1. Personal information like name, mail id, password, telephone no, etc should not be displayed on websites
2. Photograph should not be posted on social networking sites.
3. Mysterious mails and users should not be responded.
4. Alphanumeric high strength password with special symbols should be used.
5. Latest and updated antivirus should be used to secure the system and data.

CYBERCRIMES AND DIFFERENT KINDS OF CYBER OFFENCES UNDER INDIAN LAW:

The Internet is notable for two exceptional features. Cybercrime, first and foremost, has no geographical boundaries and may be perpetrated by anybody, anywhere in the globe. The second unique selling point is the anonymity it provides to its customers, which comes with pros and cons. While some see anonymity as a means to an end a platform from which they may share their unique viewpoint with the world others see it as a curse. Both the enforcement

of the law and the prevention of crime are hampered by these characteristics. Specifically, there is no law in place that addresses cyberbullying of women at this time. Most women are unaware that there are other rules that may be used in this specific situation. Most women don't even know their rights exist.

Sculptures and guidelines abound with rules that penalise digital misconduct. Most legislation, however, are based on the Indian Penal Code (IPC) and the Information Technology Act (IT Act) of 2000. Crimes in India are defined and punished according to the Indian Penal statute (IPC), the country's main criminal statute. IPC, which once dealt with rules and discipline pertaining to the real world, has been formally revised and astutely interpreted to cater to cybercriminals. Despite this, there is a specific rule governing the use of data innovation and the misuse of it known as the IT Act.

(a) Cyber-piracy When people act inappropriately when using the internet, this happens. Typically, a domain name that seems to be similar to an already popular domain, entity, or brand name is used for this purpose. Squatter is short for "squattering," and "squatted name" is short for the name that the criminal uses while committing the crime. Squatters may register the domain names they have unlawfully taken advantage of by being the first to do so. After the squatter has demanded money from the famous brand's owner for the domain that was formerly theirs, the owner has the legal right to stop the squatter from using those domains if they refuse. The "Uniform Domain Name Dispute Resolution Policy" in India and other countries' IP protections are both compromised by this kind of behaviour.

(b) The threat of cyber-anarchy First to use the term "cyber terrorism" was Barry Collin of the California Institute for Security and Intelligence, who is a Research Fellow. The merging of cybernetics with terrorism is what he calls cyberterrorism. In 2002, some prominent websites in the country began airing messages related to the Kashmir dispute, leading many to suspect that Pakistani hackers, allegedly directed by Doctor Naikar, were responsible. For India, these cyberattacks were a first. Pakistan Cyber Arm also breached the CBI website in April 2010.

(c) Theft of Data It occurs when an individual acquires or steals sensitive information that is not allowed to be publicly exposed. In 2000, the IT Act established penalties for similar infractions under Sections 43, 43A, and 66. Sections 43A and 66 address the sentencing methods, whereas Section 43 covers the offence itself. Additional cases that made use of Section 66 were Syed Assifuddin and Others v. The State of Andhra Pradesh and Others.

(d) Cyberattacks In addition to being one of the more severe infractions, it is also rather easy to commit. Any unauthorised access to, or sharing of, data stored on, or sent by, a computer, mobile device, or other electronic device is considered hacking in the broadest sense. Since hacking encompasses so many different types of crimes, it's possible that stealing someone else's email address may be considered hacking if the owner of the account inadvertently left it in login mode on a device. The number of hacking-related crimes in India is steadily increasing. Periodically, hackers have gained access to the websites of Jadavpur University, the Ministry of Defence, and a number of other notable organisations. Hacking is now considered a felony according to Section66(2) of the IT Act.

(e) Hacked websites When a someone forcefully and illegally cracks the password of a website and takes control of it, they might start modifying the content on the website. When someone illegally takes possession of a website, the rightful owner loses all authority over it. According to Indian law, Section 65 of the IT Act, 2000 deals with such actions.

(f) Acts of Cyberbullying Bullying usually involves making threats or instilling fear in another person. Intimidation or threats conducted via digital methods are known as cyberbullying. Cyberbullying, in which someone intentionally causes damage to another person via the use of electronic equipment such as computers, mobile phones, and the like, is an issue in today's society. Nearly half of all children(53%) had been victims of cyberbullying at some point in their time spent online, according to a 2011 survey by Microsoft on global youth online behaviour. After China and Singapore, India ranked third for this kind of bullying. Indian law does not provide a specific definition of cyberbullying; nonetheless, violators may face criminal prosecution under Section 66 of the IT Act of 2000.

(g) Internet Harassment The origin of cyberstalking may be traced back to online stalking. Constantly keeping tabs on another person is illegal in India and is known as "stalking" in its fullest meaning according to the country's penal code. Online platforms are used in cyberstalking. While it may not seem like a big deal to any one individual, it might infringe upon the right to privacy, which is now a fundamental right in India according to Article 21 of the constitution.

Despite Section 354D's gender specificity and its restriction to male abusers, the 2013 Criminal Law (Amendment) Act criminalises online stalking and makes it punishable under the Indian Penal Code. Although cyberstalking is not explicitly addressed in Indian law, Section 72 of the IT Act provides

guidance on how to deal with breaches of privacy and confidentiality. Since this kind of offence may be difficult to objectively define, it is more important to make reference to Section 72 of the IT Act, even if it does not specifically address digital following.

ANALYSIS OF DATA

The Indian government, the National Crime Records Bureau, and the Ministry of Home Affairs have all provided us with statistical data. Based on the number of cybercrime cases and arrests made under the Indian Penal Code and the Information Technology Act, we have examined the data and identified the states, cities, and four metro areas of India that are most at risk. In 2023, there were more cybercrime instances than in 2022, according to the statistics shown in figures 1-3. This suggests that cybercrime is on the rise throughout India's states and cities. According to the number of cybercrime instances reported in 2022 and 2023, the three most susceptible states in India are Maharashtra, Bengaluru, and Mumbai. Because the number of people arrested in 2023 is based on all cases reported up to that year, figure 1 reveals that there were more people arrested in Maharastra in 2023 than there were cases filed. On the other hand, the data (Figures 1) reveal that there was a significant decrease in the number of individuals apprehended in relation to the number of cybercrime incidents recorded in 2023. Fewer people have been taken into custody in Bengaluru and Assam compared to the number of incidents reported in 2023.

Table 1: Statistics of Cyber Crime

STATE	CASES REGISTERED IN 2012	CASES REGISTERED IN 2013
MAHARASTRA	561	307
ANDHRA PRADESH	454	651
KARNATAKA	437	533
KERALA	312	383
WEST BENGAL	309	342
UTTAR PRADESH	249	682
MADHYA PRADESH	197	342
RAJASTAN	154	297
PUNJAB	78	156
ASSAM	28	154

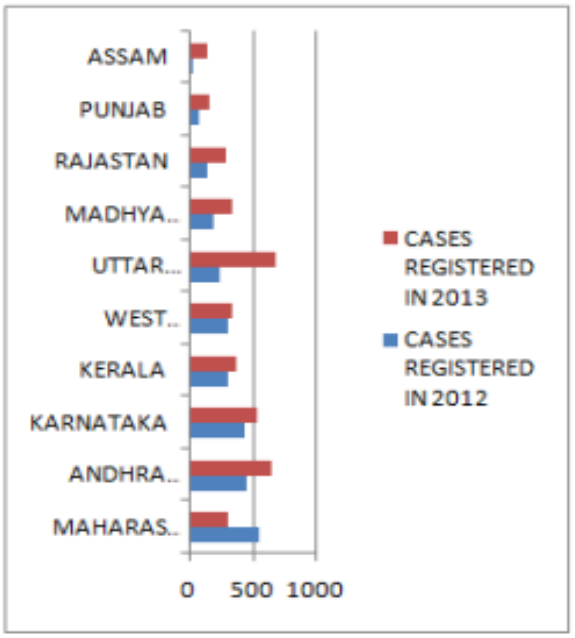

Figure 1: cyber crime cases registered

Table 2: Statistics of Cyber Crime

CITY	CASES REGISTERED IN 2012	CASES REGISTERED IN 2013
BENGALURU	349	417
VISHAKHAPATANAM	154	175
PUNE	108	100
DELHI	80	150
JAIPUR	73	131
KOLKATA	68	96
KOCHI	65	37
HYDERABAD	42	160
MUMBAI	35	132
CHANDIGARH	33	11

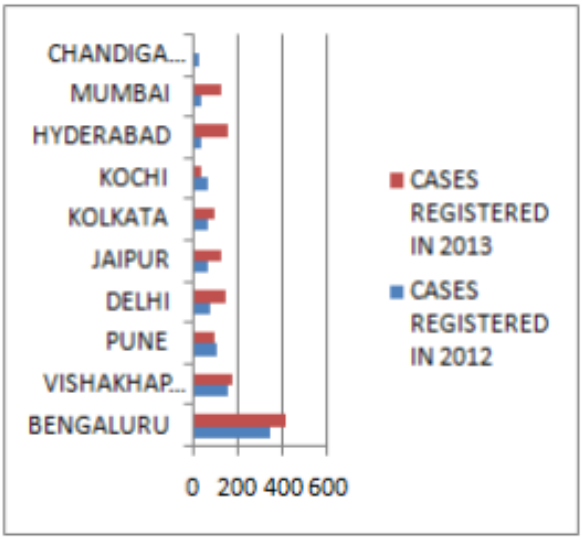

Figure 2: cyber crime cases registered

Table 3: Statistics of Cyber Crime

STATE	CASES REGISTERED	PERSON ARRESTED
MAHARASTRA	307	603
ANDHRA PRADESH	651	313
KARNATAKA	533	104
KERALA	383	169
WEST BENGAL	342	209
UTTAR PRADESH	682	602
MADHYA PRADESH	342	177
RAJASTAN	297	151
PUNJAB	156	133
ASSAM	154	2

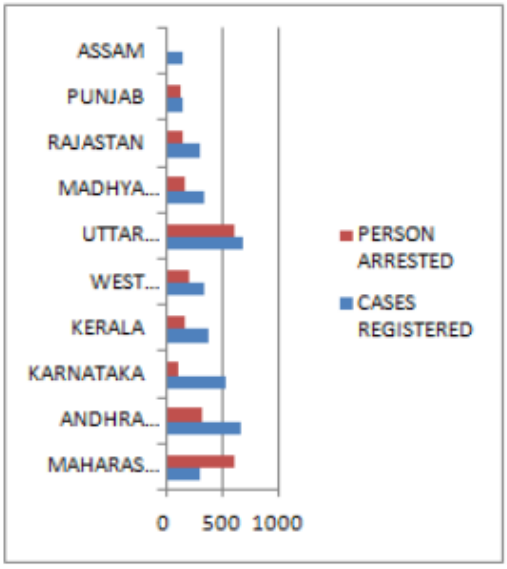

Figure 3: Persons arrested against the cyber crime cases registered

Table 4: Statistics of Cyber Crime

CITY	CASES REGISTERED	PERSON ARRESTED
BENGALURU	417	47
VISHAKHAPATANAM	175	86
PUNE	100	42
DELHI	150	45
JAIPUR	131	41
KOLKATA	96	31
KOCHI	37	11
HYDERABAD	160	87
MUMBAI	132	78
CHANDIGARH	11	9

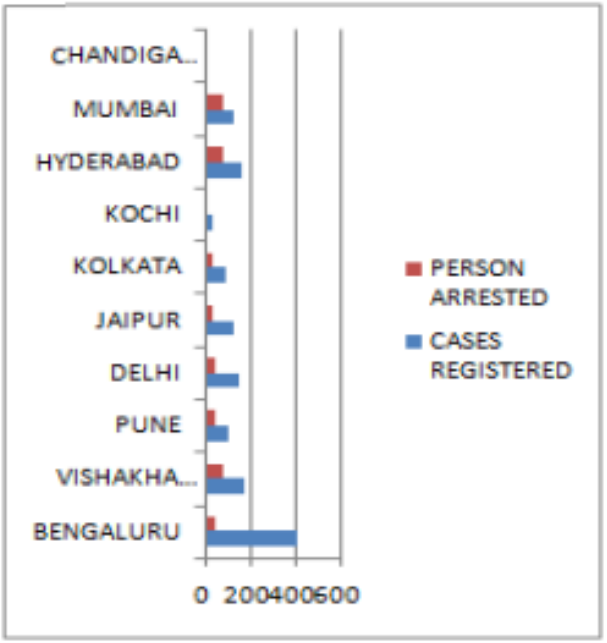

Figure 4: Persons arrested against the cyber crime cases registered

Table 5: Statistics of Cyber Crime

METROPOLITIAN CITY	CASES REGISTERED IN 2013	PERSON ARRESTED In 2013
MUMBAI	150	45
DELHI	132	31
KOLKATA	96	78
CHENNAI	13	15

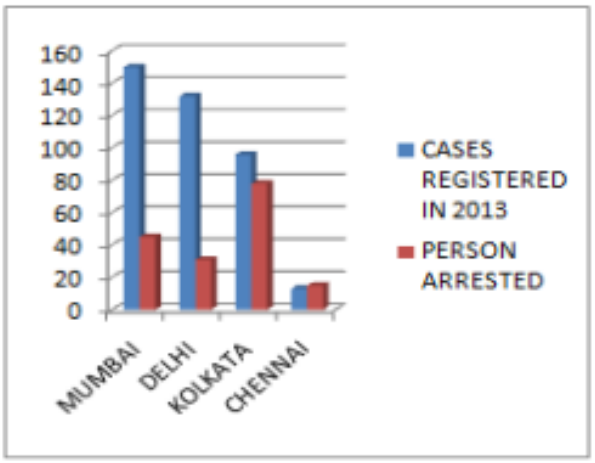

Figure 5: Persons arrested against the cyber crime cases registered

THE NEED FOR A SPECIFIC LEGAL FRAMEWORK

Given the foregoing, it is clear that the digital world presents India with its own set of problems and dangers, which is why the country needs its own cybercrime legislation. The potential for cybercrime and dangers is rising at an exponential rate due to the increasing integration of our lives into the digital world. Consequently, in order to successfully fight cybercrime, it is crucial to have thorough rules and regulations.

Cybercrime requires its own specific legal framework due to its distinct characteristics. Because cybercrime does not respect physical borders, it is more difficult to track down and bring those responsible to justice. Due to the immaterial character of digital data and the anonymity offered by the internet, certain legislative measures are necessary for the proper investigation and prosecution of cybercriminals. To ensure the safety of sensitive information, a cybercrime specific legislative framework is essential. More and more people and businesses are storing a great deal of sensitive data online because to the prevalence of online banking, e-commerce, and other digital interactions. This data is protected against abuse, loss, or unauthorised access by a strong legal framework. To protect the privacy and security of individuals' information, it lays down standards for data protection, security, and breach reporting.

Protecting the nation's security requires a well-defined set of laws. Espionage, sabotage, and assaults on vital infrastructure are all examples of cyber dangers that may jeopardise a nation's security. The government and law enforcement authorities are able to effectively confront these dangers because of a specific legislative framework. It sets up procedures for information exchange and collaboration amongst different parties, as well as rules for responses and preventative actions. With this system in place, the nation can be confident that it is ready to deal with cyber events that might threaten its security.

The capacity of law enforcement to combat cybercrime is bolstered by a particular legislative framework. Expertise, equipment, and methods tailored to the investigation of cybercrime are essential. Law enforcement authorities are better able to gather evidence, investigate cyber events, and prosecute criminals when they have clear legal authority, protocols, and regulations to follow. Through the establishment of channels for mutual legal aid and extradition, it also facilitates international collaboration in the fight against cybercrime. Therefore, in order to tackle the ever-changing threats presented by the digital world, India needs a cybercrime legislation. It protects sensitive information, strengthens law enforcement, promotes international collaboration, and keeps the country secure. In order to protect its residents and businesses from cybercrime, India has to establish stringent cyber laws and regulations.

CONCLUSIONS

In this study, we have shown how cybercrime poses serious problems for Indian law enforcement and how quickly we need a new legislative framework to deal with this issue. Finding out how cybercrime has become the most common kind of crime in India has been the major focus of this investigation. This study asserts that in this technologically advanced era, several forms of cybercrime are prevalent. The number of cybercrime cases in various Indian regions and localities has been steadily rising over the last decade, according to the analysis. Compared to the amount of reported cybercrimes, the number of people apprehended is shockingly low. Our Information Technology Act cannot guarantee total security for our cyber world, hence it is evident that there are still unresolved difficulties with our cyber frameworks and Indian cyber laws. Cyber rules, together with knowledge and good policymaking, are so necessary. India can make the internet a safer place for its residents and businesses by taking on cybercrime head-on and solving its legal problems. To combat the increasing threat of cybercrime in India, it is critical that lawmakers, stakeholders, and policymakers collaborate to create and execute a strong legislative framework.

REFERENCES

1. Umejiaku and Anyaegby, (2016), "Legal Framework for the enforcement of cyber law and cyber ethics in Nigeria", International Journal of Computers and Technology, Vol-15, No.10.

2. Kaur, M., Saini, M. (2023), Indian government initiatives on cyberbullying: A case study on cyberbullying in Indian higher education institutions. *Educ Inf Technol* 28, 581–615. https://doi.org/10.1007/s10639-022-11168-4

3. Misra, A., Chacko, M. (2021), Square pegs, round holes, and Indian cybersecurity laws. *Int. Cybersecur. Law Rev.* 2, 57–64. https://doi.org/10.1365/s43439-021-00026-7

4. Ajoy P.B (2022). Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis. Sch Int J Law Crime Justice, 5(2): 74-79.

5. Kethineni, S. (2019). Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. In: The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-90307-1_7-1

6. Anil Lamba, 2014. "Uses Of Cluster Computing Techniques To Perform Big Data Analytics For Smart Grid Automation System", International Journal for Technological Research in Engineering, Volume 1 Issue 7, pp.5804-5808,2347-4718.

7. R. P. Kaur, Statistics of cyber crime in India: An overview, International journal of Engineering and Computer Science, vol.2, issue8, pp.2555-2559, 2013.

8. R.S. Patel, D. Kathiria, Evolution of cyber crime in India, International Journal of Emerging Trends and Technology in Computer science,vol.2,issue 4,pp.240- 243,2013.

9. Gercke, M. (2012). Understanding Cybercrime: Phenomena, Challenges and Legal Response (1st ed.). International Telecommunication Union. https://www.itu.int/ITUD/cyb/cybersecurity/docs/Cybercrime legislation EV6.pdf

10. Smith, John. "Legal Implications of Artificial Intelligence: A Comparative Analysis." Journal of Cyber Law, vol. 25, no. 2, 2020, pp. 45-63.

11. Verma, Shikha. "Capacity Building for Legal Professionals in the Cyber Age." Journal of Legal Education and Practice, vol. 21, no. 2, 2017, pp. 123-140.

12. Saurabh Tewari China's Cyber Warfare Capabilities, USI Journal, April 2019 – June 2019, accessed at https://usiofindia.org/publication/usi-journal/chinas-cyber-warfarecapabilities/

13. Atrey, Ishan, Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence (July 9, 2023). International Journal of Research and Analytical Reviews, July 2023, Volume 10, Issue 3 .

14. Goldstone, D., & Shave, B.-E. (2018). International Dimensions of Crimes in Cyberspace. Fordham International Law Journal, 22(5), 1924–1971.

15. Jetha, K. (2013). Cybercrime and Punishment: An Analysis of the Deontological and Utilitarian Functions of Punishment in the Information Age. ADFSL Conference on Digital Forensics, Security and Law, 15–20.

Corresponding Author

S. Nakkeeran*

Research Scholar, University of Technology, Jaipur, Rajasthan, India

Email: advocatekeeran@gmail.com