EVOLVING CYBER OFFENCES AND THE ROLE OF STATE MACHINERY IN SAFEGUARDING DIGITAL BORDERS: LEGAL FRAMEWORKS, CHALLENGES, AND SOLUTIONS FOR A NEW ERA

Himanshi, LLM (Criminal), SRM University, Delhi NCR[1]

ABSTRACT

As the world races towards a future dominated by technology and artificial intelligence, a critical challenges emerges to safeguarding the wisdom held within traditional systems. This paper, titled "*Evolving cyber offences and the role of state machinery in safeguarding digital borders: Legal frameworks, challenges, and solutions for a new era*," delves into the existing frameworks and proposes solutions for their improvement.

Cybercrimes have evolved as a complex phenomenon in the current digital era, presenting major risks to people, organizations, and countries. The virtual world is rife with threats that need prompt and efficient legal action, ranging from identity theft and financial fraud to cyber terrorism and data breaches. The judicial institutions and state processes in charge of upholding the law must change along with the nature of crime and technological advancements. Increasing significance of cybersecurity in all facets of contemporary life including governments and societies is the driving force behind the topic selection. India confronts particular risks that need for a strong and flexible legal framework. India has quickly growing digital environment and rising internet usage as government promoting digital transactions through various schemes. But there are still large gaps in international collaboration, knowledge, and enforcement despite legislative initiatives like the Information Technology Act of 2000.

This paper critically examines existing cyber offence prevention regimes, dissecting their strengths and weaknesses, and explores innovative approaches to address the shortcomings. The focus extends beyond legislation, delving into practical implementation and the power of international cooperation to foster a more inclusive and equitable system.

Keywords: Cyber Offence, Investigation, Cyberthreats, Cyber Security, Stakeholders, Technology

[1] Himanshi, LLM (Criminal) Student at SRM University Delhi - NCR

1. INTRODUCTION

The issue of cybercrime in India is extremely important because of the nation's rapidly growing internet user population and digital transformation, both of which have made it more vulnerable to cyberattacks. Cybercrimes including hacking, phishing, identity theft, online fraud, cyberbullying, and cyberterrorism have increased in frequency and complexity as more people, companies, and government services move online.[2]

Understanding and successfully addressing these crimes is crucial because they represent serious hazards to national security, vital infrastructure, financial stability, and personal privacy. Strong regulatory frameworks and enforcement procedures are desperately needed to protect India's digital environment, as evidenced by the growing number of incidents and the significant financial and societal effects of cybercrime.[3]

In order to combat cybercrime in the nation, the governmental apparatus plays a crucial role. According to the constitution, state governments are in charge of stopping, looking into, and prosecuting cybercrimes that occur inside their borders. To effectively manage cyber investigations, they run specialized cybercrime cells with highly skilled staff and cutting-edge equipment.[4]

The central government agencies, which offer technical assistance, strategic guidance, and platforms like the "National Cyber Crime Reporting Portal" to expedite complaint registration and case management, collaborate closely with the state apparatus.

Through this cooperative framework, state authorities take part in national initiatives to improve cybersecurity awareness, capacity building, and quick reaction to new cyberthreats in addition to enforcing cyber laws locally.

2. Literature Review

Dr. Pavan Duggal's book **Cyberlaw: The Indian Perspective (3rd Edition, LexisNexis, 2023)** provides a detailed review of India's Information Technology Act, 2000, and its revisions. He discusses the Act's merits and weaknesses in dealing with modern cyber dangers, emphasizing the importance of ongoing legislative development to keep up with technical

[2] N.S. Nappinai, *Technology Laws Decoded* p.45-68 (LexisNexis, 1st Edition, 2017).

[3] Badruddin and Anis Ahmad, "Cyber Security Challenges: Some Reflections on Law and Policy in India" 1(1) *The Haryana Police Journal* 1-9 (2017).

[4] Adv. Prashant Mali, *Cyber Law and Cyber Crimes Simplified* p. 110-132 (5th Edition, Cyber Infomedia, 5th Edition, 2018)

improvements.[5]

The convergence between cyber law and developing technology is thoroughly examined in **Dr. Jyoti Rattan**'s **Cyber Laws, Information Technology & Artificial Intelligence (10th Edition, Bharat Law House Pvt. Ltd., 2024).** She highlights the complexity brought about by the integration of technology into daily life by talking about anything from malware and network security to the effects of artificial intelligence on legal systems.[6]

Technology Laws Decoded (1st Edition, LexisNexis, 2017) by N.S. Nappinai explores the relationship between technology and a number of legal areas, such as criminal law, intellectual property, and constitutional law. She promotes a comprehensive approach to cyber law that takes into account both substantive and procedural factors, highlighting the procedural difficulties presented by electronic evidence and jurisdiction in cyberspace.[7]

The rise in cybercrimes in the quickly changing digital ecosystem makes a thorough grasp of cyber laws and the defenses against these threats essential. **"Cyber Law and Cyber Crimes Simplified" (5th Edition, Cyber Infomedia, 2018)** by **Adv. Prashant Mali** is a seminal work that clarifies the intricacies of cyber law in India. The goal of the book is to demystify the topic so that both laypeople and legal experts interested in the field of cyber security may understand it.[8]

A thorough analysis of India's cyber law environment is provided in **Kant Mani's Legal Framework on Cyber Crimes (3rd Edition, Kamal Publishers, 2023)**, with an emphasis on the Information Technology Act, 2000 and its ensuing revisions. The book explores the procedural issues of adjudicating cybercrimes, the subtleties of cyberspace, and the admissibility of digital evidence. The Information Technology (Intermediaries Guidelines) Rules, 2011 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 are two notable examples of the comprehensive appendices that include pertinent rules and regulations. Because of its methodical approach, it is a useful tool for academics, students, and legal professionals who want to comprehend the complexities of Indian cyber law.[9]

[5] Dr. Pavan Duggal, *Cyberlaw: The Indian Perspective* p. 121-134 (LexisNexis, 3rd Edition, 2023).

[6] Dr. Jyoti Rattan, *Cyber Laws, Information Technology & Artificial Intelligence* p. 34-89 (Bharat Law House Pvt. Ltd., 10th Edition, 2024).

[7] N.S. Nappinai, *Technology Laws Decoded* p.45-68 (LexisNexis, 1st Edition, 2017).

[8] Adv. Prashant Mali, *Cyber Law and Cyber Crimes Simplified* p. 110-132 (5th Edition, Cyber Infomedia, 5th Edition, 2018).

[9] Kant Mani, *Legal Framework on Cyber Crimes* p. 114- 152(Kamal Publishers, 3rd Edition, 2023).

3. Research objectives

- To examine new trends and developments in technology that make it possible for more recent types of cybercrimes to occur, paying particular attention to how these threats change in both urban and rural areas.
- To examine how the public and police engage throughout the reporting and settlement of cybercrimes, paying particular attention to victim assistance, accessibility, and grievance redressal procedures.
- To assess how well various law enforcement and judicial agencies coordinate their efforts to combat interstate or cross-border cybercrimes.

4. Research questions

- How effective are state police forces and specialized cybercrime units in addressing and mitigating cybercrime across India?
- How well do current legal frameworks, such as the Information Technology Act of 2000, meet the intricacies of cybercrime, and what changes are needed to improve their effectiveness?
- How can public awareness efforts and digital literacy programs help to reduce cybercrime victimization in distinct Indian states?
- What are the important takeaways from state-level cybercrime case studies, and how might these insights be used to shape future cybercrime policies and practices?

5. Research Methodology

An extensive doctrinal legal examination of current legislation, legal systems, and judicial precedents forms the foundation of this research. This study uses a socio-legal perspective to acknowledge that cybercrime is a problem that is profoundly ingrained in social reality rather than only being a technical or legal one.

This paper will use in-depth case investigations to bring theoretical analysis closer to practical application. This paper will offer a thorough and comprehensive knowledge of how cybercrime is changing throughout Indian states and how well-equipped the state apparatus is to respond by utilizing this multi-layered and multidisciplinary technique. The combination of doctrinal, socio-legal, and case-based methodologies guarantees that the study not only adds to scholarly discussions but also provides significant, useful suggestions for administrative action, policy enhancement, and legal change.

6. Legal Framework Governing Cyber Crimes in India

In India, the law relating to cyber crimes has come to conform to the increasing threat posed by abuse of digital media. Realizing the necessity for specialized legislation to combat offences such as hacking, identity theft, cyber stalking, breach of data, fraud through the internet, and the dissemination of obscene or defamatory matter, the Indian legislature enacted and amended various provisions of statutes.

In addition to the Information Technology Act, traditional legal codes like the Indian Penal Code of 1860 and sector-specific regulations have been employed to strengthen the legal recourse against cyber attacks. Court judgments, government orders, and global coordination have also made major contributions towards putting together a comprehensive legal framework with the aim of encouraging cybersecurity, protecting digital rights, and punishing cybercrime.[10]

6.1 Constitutional provisions related to cyber law

India has made strides in the last two decades toward a digital economy, which is defined by online communication, mobile technology, and the internet. The most notable legal issues brought forth by this digital transformation are those pertaining to cybersecurity and data privacy. As online transactions, data creation, and electronic communications have increased, so too have worries about the gathering, processing, and abuse of sensitive personal data. This has sparked a constitutional discussion over data privacy.[11]

Although “data privacy” and “cyber law” are not expressly mentioned in the Indian Constitution, the Supreme Court and other judicial authorities have interpreted them to include the protection of information as a crucial basic right. Through historic decisions and growing legal theory, the Indian constitutional framework has increasingly evolved to address the consequences of data abuse and cyber risks in the digital age.[12]

Article 21[13], which stipulates that “No person shall be deprived of his life or personal liberty except according to procedure established by law,” serves as the foundation for this fundamental safeguard. Originally, this phrase was interpreted strictly as meaning primarily bodily liberty. However, the Supreme Court has read Article 21 in a significantly broader

[10] J.W.C. Turner, *Kenney’s Outlines of criminal law* 17 (University Press, Cambridge, 19th Edition, 1966).

[11] Talat Fatima, *Cyber Crime* 64-68 (Eastern Book Company, Lucknow ,1st Edition, 2011).

[12] Varshney, R. and Kapoor, “Cybersecurity & constitutional implications: A study of gaps in Indian legal provisions” 2(1) *Journal of Cybersecurity* 78-95(2017).

[13] The Constitution of India, art. 21.

context throughout the years, recognizing it as a source of various unenumerated rights necessary to live a dignified and free life. Among these, the right to privacy has been deeply embedded as a component of personal autonomy.[14]

The doctrine on the right to privacy began to shift in judgments such as “Kharak Singh v. State of Uttar Pradesh”,[15] in which the Court addressed the legitimacy of police monitoring. Although the majority judgment did not directly support the right to privacy, Justice Subba Rao's dissenting opinion stated unequivocally that unwanted interference into a person's private life was illegal. This opposition eventually served as the philosophical underpinning for India's privacy rights.

Articles 14, 19, 21, and 32 provide a strong constitutional basis for protecting personal data in the digital era. They guarantee that people have the right to privacy and legal remedy if their privacy is violated. The Supreme Court's role in interpreting these rights and defining privacy as a fundamental right in the historic Puttaswamy decision was particularly noteworthy. This decision set essential standards that must be followed in any law or government action affecting an individual's privacy, including legality, need, and proportionality.[16]

6.2 Offences under IPC and BNS

1. Theft and possession of cell phones or stolen data:

IPC Section 379 stipulates that theft of mobile phones or data carries a maximum sentence of three years in jail, a fine, or both. If someone intentionally steals digital property (such data or gadgets), they are subject to IPC Section 411. The BNS equivalent for stealing is Clause 303, while the BNS equivalent for receiving stolen property is Clause 314. Comparable penalty systems are maintained in both clauses.[17]

2. Cyber theft and data breaches:

Cyber theft, often known as data theft, is covered by both Section 66 of the IT Act of 2000 and Section 379 of the IPC. In situations involving computer theft or unauthorized access to data, these provisions are essential. Like theft and misappropriation, these activities are nevertheless

[14] Dr. Pavan Duggal, *Cyberlaw: The Indian Perspective* p. 121-134 (LexisNexis, 3rd Edition, 2023)
[15] (1964) 1 S.C.R. 332
[16] Vaishnavi Bansal and Dr. P.S. Panwar, “Cybersecurity And Data Privacy: A Constitutional Analysis Of India's Response To Cyber Threats” 12(8) *International Journal of Creative Research Thoughts* 940-951 (2024).
[17] Gayathri. V, “How ‘IPC’ Goes Hand in Hand with ‘IT Act’ in Dealing with Cyber Crimes” 4(4) *International Journal of Research Publication and Reviews* 1198-1205 (2023).

prohibited by BNS's own rules.

3. Privacy Invasion:

Both Section 66E of the IT Act and Section 292 of the IPC (obscenity) forbid capturing or sharing images of a private location without authorization. These will continue under similar themes in the BNS through provisions related to obscenity and infringement of privacy.[18]

4. Sending disrespectful or threatening communications

Sections 500 through 509 of the IPC deal with insults to modesty, slander, and threats. These are used when communications are conveyed through digital communication systems. These parts are comparable to clauses 356 to 360 of the BNS; the punishments are the same, but the wording is a little different.

6.3 Digital Personal Data Protection Act of 2023

In India, the gathering, storing, and use of digital personal data are governed under the “Digital Personal Data Protection (DPDP) Act”.[19] It may be used when digital personal data is immediately acquired; second, it can be used when physical data is first obtained and then converted to digital format. However, if personal data is solely stored in physical (as opposed to digital) form, the Act is not applicable.The DPDP Act also has extraterritorial applicability. This suggests that it could apply to companies based outside of India that manage Indian residents’ digital personal data in order to provide products or services. However, the Act doesn't address whether it protects the data of Indian residents living abroad or non-citizens in India.[20]

The DPDP Act is considered a foundational piece of legislation in India's efforts to regulate digital privacy.Unlike the earlier “Information Technology (IT) Act”, this law clearly defines what personal data is and what constitutes a breach of personal data, including sharing, illegal access, and data deletion. With a few exceptions, it states that processing data without an individual's consent is prohibited.[21]

[18] Mrs. K. Kalisel, “Cyber crime under the provisions of IPC” 11(11) *IJFANS International Journal of Food and Nutritional Sciences* 1137-1152 (2022).

[19] The Digital Personal Data Protection (DPDP) Act, 2023 (Act 113 of 2023).

[20] Charru Malhotra and Udbhav Malhotra, “Putting Interests of Digital Nagriks First: Digital Personal Data Protection (DPDP) Act 2023 of India” 70(3) *Indian Journal of Public Administration* 516-531 (2024).

[21] Subhajit Saha and Surjashis Mukhopadhyay, “A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023” 10(1) *International Journal of Law and Social Sciences* 84-95 (2023).

7. Cyber Crime Investigation and Enforcement Agencies

7.1 "The Indian Cybercrime Coordination Center (I4C)":

"The Indian Cyber Crime Coordination Centre (I4C)", the top national organization for combating cybercrime, was established in 2020 under the "Ministry of Home Affairs (MHA)." It is in charge of establishing a national cybercrime reporting portal, coordinating law enforcement activities among several states, and promoting research and capacity building in the fields of digital forensics and investigation.

One important I4C initiative is the "National Cyber Crime Reporting Portal" (www.cybercrime.gov.in), which enables citizens to report cybercrimes, particularly those involving women and children.[22]

7.2 "Ministry of Home Affairs' Cyber and Information Security (CIS) Division":

The MHA's CIS Division is in charge of developing and implementing policies related to infrastructure development, cybercrime prevention, and cybercrime training. In addition to supporting state police forces with funding and technical assistance for the establishment of cybercrime cells, it plays a significant role in national policymaking.

7.3 "The Cyber Crime Division of the Central Bureau of Investigation (CBI)":

The top investigative organization in India, the CBI, has a "Cyber Crime Investigation Cell." It looks into well-known cases of corporate data theft, online fraud, hacking, and financial scams, particularly those with interstate or global ramifications. In cases involving cross-border cybercrime, the CBI also works with Interpol.[23]

7.4 "CERT-In, the Indian Computer Emergency Response Team"

The national nodal agency for handling cyber security incidents is CERT-In, which is a division of the "Ministry of Electronics and Information Technology (MeitY)." It provides early warnings, issues security alerts and advisories, and tracks, gathers, and shares information on cyberthreats. In order to manage and contain threats, CERT-In collaborates with ISPs, businesses, and other government agencies and supports post-event analysis.[24]

[22] P. Narmadha and N. Sudalaimuthu, "Cybercrime Investigation and Digital Forensics: A Study of the Tools and Techniques for Investigating Organized Crime Groups" 8(10) *ICONIC research and engineering journals* 519-525 (2025).

[23] Sarita Sitaraman, "Four New Cyber Crime Prevention Initiatives Launched in India," LinkedIn, https://www.linkedin.com/pulse/four-new-cyber-crime-prevention-initiatives-launched-india-jwt7f/ (published September 19, 2024, accessed May 20, 2025).

[24] Kevin F. Steinmetz and Brian P. Schaefer, "Exploring Cybercrime Capabilities: Variations Among

7.5 "Cyber Police Stations and State Cyber Crime Cells":

To look into local-level cybercrimes, each Indian state has set up Cyber Crime Cells and designated "Cyber Police Stations." These units have trained staff and cyber forensic tools to handle crimes like data theft, phishing, online harassment, and social media abuse. States like Telangana, Karnataka, and Maharashtra have established specialized rapid response teams and cybercrime labs.

8. Case studies: examining the trends in new era

The rapidly evolving digital ecosystem has brought about major changes in the type and extent of cybercrimes. The new era of cybercrimes is characterized by the emergence of organized cybercriminal networks, the complexity of assaults, and the widespread use of automation and artificial intelligence to exploit vulnerabilities. In contrast to the previous forms of cybercrime, which were mostly limited to hacking or email scams, the current cybercrime ecosystem has expanded to encompass sophisticated threats such as ransomware assaults, cryptocurrency scams, data breaches, deepfakes, cyberbullying, and online radicalization.[25]

One of the most common trends is ransomware attacks, in which thieves encrypt a victim's data and demand payment (usually in cryptocurrency) to unlock it. These assaults, which cause major disruptions and financial losses, are no longer limited to people; they increasingly frequently target governments, healthcare systems, educational institutions, and vital infrastructure. The colonial pipeline assault in the United States in 2021 and similar instances in India show how susceptible critical systems are to hacking.[26]

8.1 Financial frauds

Online monetary fraud, according to "The World Bank (2021)", is financial fraud that happens when someone illegally obtains money or assets through technology-enabled means. Additionally, it claims that because digital networks are global, online financial fraud is becoming a bigger threat, so people should exercise caution and awareness when communicating electronically about their money.[27]

Cybercrime Investigative Units" 35(4) *Criminal Justice Policy Review* 194-215 (2024).

[25] ET Bureau, "Digital economy to grow almost twice as fast as overall economy: MeitY", *The Economic Times,* Jan 23, 2025, *available at* <https://economictimes.indiatimes.com/news/india/digital-economy-to-grow-almost-twice-as-fast-as-overall-economy-meity/articleshow/117466401.cms?from=mdr>(last visited on Mar. 28, 2025).

[26] Juneed Iqbal and Bilal Maqbool Beigh, "Cybercrime in India: Trends and Challenges" 6(12) *International Journal of Innovation & Advancement in Computer Science* 2347-8616 (2017).

[27] Asalah F Altwairqi, "Four Most Famous Cyber Attacks for Financial Gains" 9(2) *International Journal of Engineering and Advanced Technology (IJEAT)* 2131-2139 (2019).

"State Bank of India v. Pallabh Bhowmick & Ors."[28]

The Supreme Court upheld SBI's duty to compensate victims of internet frauds in January 2025, when the victim was duped by a phone call posing as a customer support agent. The fraud, which involved unlawful withdrawals after the victim downloaded a rogue app, brought attention to the risks associated with phone-based authentication issues. The decision upheld banks' duties to protect customers from these kinds of frauds.[29]

Sharat Babu Digumarti v. Government of NCT of Delhi[30]

The court ruled that electronic broadcasts of obscenity were covered by the IT Act rather than the Indian Penal Code. Within its authority, the ruling creates a precedent that is persuasive or binding.

"Poona Auto Ancillaries Pvt. Ltd. v. Punjab National Bank"[31]

When a phishing attempt resulted in a false withdrawal of ₹80.10 lakhs because the bank failed to do adequate security measures, the court imposed compensation.

8.2 Deepfake, online harassment and identity theft

Celebrities are particularly affected by deepfakes because they have a lot of publicly available information. Celebrities have the legal right to control their name, likeness, and image. Unauthorized exploitation of a person's persona occurs when they use their voice, images, and videos for commercial purposes without their consent, such as making changes using Deepfakes. As was decided in numerous recent cases, those who abuse and illegally profit from the distinctive qualities associated with the celebrity may face legal repercussions for this violation of their personality rights.[32]

The Supreme Court of India used the Hicklin test, a criterion created in Victorian England, to define obscenity in the landmark decision of "**Ranjit Udeshi v. State of Maharashtra".**[33] This criteria determined that something was considered obscene if it may corrupt or deprave those whose brains were open to immoral influences. This meant that rather than using the

[28] Special Leave Petition (Civil) No. 30677/2024.
[29] Patil Rachana Yogesh and Devane Satish R, "Backtracking Tool Root-Tracker to Identify True Source of Cyber Crime" 171 *Procedia Computer Science* 1120-1128 (2020).
[30] (2017) 2 SCC 18.
[31] (2022) 02 TDSAT CK 0045.
[32] IALM Academy, "Cyber Crime in India: Legal Hurdles and Challenges," https://ialm.academy/blog/cybercrime-in-india-legal-hurdles-and-challenges (published January 1, 2013, accessed May 20, 2025).
[33] 1965 (1) SCR 65 SC.

perspective of an average member of society, the evaluation of obscenity was conducted from the perspective of a particularly susceptible or impressionable person. By limiting freedom of expression under Article 19(1)(a) of the Constitution, this test's adoption resulted in a wide and frequently conservative view of obscenity.

8.3 Targeted harassment/ Online defamation

Defamation under Section 499[34] of the Indian Penal Code is where any individual, by words either spoken or written, signs, or visible representations, makes or conveys any statement or imputation concerning another person with the purpose of causing harm, or with the knowledge or having reason to believe that it will cause harm, such person's reputation save as mentioned in the exceptions in the section.[35]

9. Innovative Solutions and Mechanisms Adopted by States

Karnataka:

Karnataka is particularly susceptible to insider attacks and data breaches since Bengaluru is a major international center for IT. Complex cyber events involving private company information have required the state's Cyber Crime Unit to respond. A significant data breach involving the leakage of client information was announced by an IT company in 2019. According to the inquiry, an insider sold information to outside hackers, which resulted in the breach. The offender was apprehended and the stolen material was recovered as a result of prompt cooperation between the police and the company’s cybersecurity staff. This case demonstrated the dangers presented by internal actors and the value of cooperation between the police and the corporate sector.[36]

In 2019, Karnataka Police dealt with a data breach at an IT company in Bengaluru where sensitive data was leaked due to insider participation. Even with the use of AI and machine learning for predictive security, handling disputes over foreign jurisdiction remained a significant obstacle, especially when the data breach had cross-border ramifications. Due to its extensive and sometimes unrecoverable digital presence, recovering stolen or encrypted material that has been shared online has proven to be incredibly difficult.

[34] The Indian Penal Code,1860 (Act 45 of 1860), s.499.

[35] Sudhir Kumar, “Online Defamation in the Digital Age: Issues and Challenges with Particular Reference to Deepfakes and Malicious Bots” 2(8) *International Journal of Law and Policy* 32-41 (2024).

[36] Karali Y and Panda S., *et. al*, “Cyber Crime: An Analytical Study of Cyber Crime Cases at the Most Vulnerable States and Cities in India” 5(2) *International Journal of Engineering and ManagementResearch (IJEMR)* 2394-6962 (2015).

Tamil Nadu:

Due in major part to growing internet usage and fast digitalization, investment frauds and online scams have proliferated in Tamil Nadu, particularly in cities like Chennai. To adequately address these concerns, the state formed the "Tamil Nadu Cyber Crime Unit (TNCU)."[37] Scammers used social media and counterfeit websites to entice individuals with phony investment schemes in 2020. A sizable amount of the stolen money was recovered by the TNCU after they looked into the scam and detained the perpetrator. This instance illustrated the importance of public complaint redressal procedures and technical inquiry in fostering confidence among internet users.[38]

"The Tamil Nadu Police had to deal with a significant internet financial scam in 2020. Although response methods were strengthened with the establishment of the "Tamil Nadu Cyber Crime Unit (TNCU)" and cooperation with banks, the state's cybercrime investigation resources were overburdened by the large number of fraud cases it was dealing with. The challenge of tracking offenders utilizing fictitious identities and numerous digital traces dispersed over different sites was another significant issue that hampered effective investigation and conviction.[39]

Delhi:

"Delhi, the nation's capital, is vulnerable to a variety of cybercrimes, from online harassment to data theft. Addressing such challenges, particularly those that target vulnerable communities, has been made possible in large part by the "Delhi Police's Cyber Crime Unit." Numerous incidents of internet harassment and cyberbullying targeting young women were documented in 2021. The police conducted awareness campaigns to inform the public about cyber hygiene and reporting procedures, worked with social media companies, and employed digital monitoring techniques to find the offenders. The strategy was a model for urban cyber policing as it included community engagement and enforcement.[40]

Delhi Police's capacity to work with social media providers and aggressively monitor abusive content was made clear by the 2021 Cyberbullying and Online Harassment case. Dealing with

[37] Sreeya B., "Public Awareness on Cyber Crime with Special Reference to Chennai" 9(1) *International Journal of Innovative Technology and Exploring Engineering* 3362-3364 (2019).

[38] Mokha, A. K, "A study on awareness of Cyber Crime and security" 8(4) *Research Journal of Humanities and Social Sciences* 459-464 (2017).

[39] P. Datta and R. K. Kaushal, "A Technical Review Report on Cyber Crimes in India"11(2) *International Conference on Emerging Smart Computing and Informatics (ESCI), Pune*, 269-275 (2020).

[40] Seema Goel, "Cyber-Crime: A Growing Threat to Indian Banking Sector" 5(12) *International Journal of Science Technology and Management* 2394-1537 (2016).

jurisdictional concerns when trying to acquire user data from international social media platforms which are sometimes shielded by strict privacy laws was one of the most urgent obstacles, though.” Cyberbullying instances also presented legal challenges, especially when it came to striking a balance between protecting people's privacy and guaranteeing public safety.[41]

Maharashtra:

Mumbai is the financial hub of India, hence cybercrimes like ransomware attacks and financial frauds are common in Maharashtra. “The Cyber Crime Investigation Cell (CCIC)” was deliberately established by the state police to handle complex cybercrimes. A Mumbai hospital was the target of a ransomware assault in 2022 that encrypted private patient information and demanded ransom payments. Together with foreign cybersecurity organizations, the “Maharashtra Cyber Cell” was able to decrypt the data, capture the perpetrators, and restore system integrity. The event made clear how urgently high-tech digital reaction units and international collaboration are needed.[42]

“In 2022, a ransomware assault on a hospital in Maharashtra, a target-rich region like Mumbai, exposed a number of operational problems. The challenge of identifying cybercriminals utilizing anonymous networks operating from foreign places constituted a significant concern, even with the Cyber Crime Investigation Cell (CCIC) and international collaboration (e.g., with Interpol).” The investigation procedure was both complicated and time-sensitive since it required balancing the requirement to preserve digital evidence with the necessity to respond quickly during a ransomware attack.

10. Role of Central-State Collaboration

Since cyberthreats transcend national borders and necessitate a coordinated response, India's Central and State governments must work closely together to tackle cybercrimes. By creating and overseeing vital organizations that offer national supervision, strategic direction, and technology infrastructure, the Central Government performs a crucial role. “The Indian Cyber Crime Coordination Centre (I4C)”, a nodal organization created to coordinate operations among different law enforcement agencies (LEAs) around the nation, is one of the important

[41] PTI, “Delhi Police draws strategy to curb digital arrest frauds, online complaint platform in works”, *Hindustan Times*, May. 17, 2025, *available at* <https://www.hindustantimes.com/india-news/delhi-police-draws-strategy-to-curb-digital-arrest-frauds-online-complaint-platform-in-works-101747482523149.html > (last visited on May. 17, 2025).

[42] Cecelia Horan and Hossein Saiedian, “Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions” 1(4) *Journal of Cybersecurity and Privacy* 580-596 (2021).

organizations. To facilitate efficient monitoring and prompt reaction to cybercrime situations, the I4C provides a complete platform that integrates data analytics, information sharing, and complaint registration.[43]

"The National Cyber Crime Reporting Portal (NCRP)", which is run by the Central Government, also enables anyone to immediately report cybercrimes, including financial scams. In order to ensure that cases are monitored and handled quickly, these complaints are thereafter forwarded to the appropriate State or Union Territory law enforcement agencies for additional investigation and action.[44] Another significant project of the center is the Central Suspect Registry, which compiles information on cybercrime suspects from every state into a single database. This database aids in the identification of repeat criminals and promotes interstate collaboration in order to prevent and resolve crimes.[45]

Through the creation of the "Cyber Fraud Mitigation Centre (CFMC)", the Central Government's responsibility is further expanded to include specialized cybercrime fields such as financial scams. In order to coordinate the quick identification and mitigation of cyber financial crimes, this center brings together officials from banks, telecom providers, IT intermediaries, and law enforcement..[46] Through organizations like CERT-In (Indian Computer Emergency Response Team) and the Ministry of Electronics & Information Technology, the government authorities offer vital financial support, capacity building, and timely warnings on changing cyber threats in addition to operational support.

11. Conclusion

The twin imperatives of preventing cybercrime and protecting individual privacy have become crucial issues as India enters a new era characterized by technological innovation. The breadth and effect of cyber risks have been greatly expanded by the growing integration of digital technology into daily life, from financial transactions and governance to personal communication. The cyber realm has evolved into a place of both opportunity and danger, where people, companies, and the government are always at risk from nefarious activities like

[43] Hannarae Lee and Hyeyoung Lim, "Awareness and Perception of Cyber Crimes and Cyber Criminals" 2(1)*International Journal of Cybersecurity Intelligence & Cybercrime* 1-3 (2019).

[44] Supriya, R. and Tyagi, M. S. et.al, "Cyber Crimes in India: A Critical Analysis" 7(6) *International Journal of Mechanical Engineering* 304- 312. (2022).

[45] Er. Navneet Kaur, "Introduction of Cyber Crime and its Type" 5(8) *International Research Journal of Computer Science* 435- 439 (2018)

[46] Rajya Sabha Unstarred Question No. 225 on November 27, 2024 *available at:* https://www.mha.gov.in/MHA1/Par2017/pdfs/par2024-pdfs/RS27112024/225.pdf (last visited on Mar. 03, 2025).

ransomware, phishing, cyberstalking, sextortion, identity theft, and massive data breaches.

Although the Information Technology Act of 2000 was the primary piece of legislation that governed cyber activity in India, its framework is now woefully unable to handle the intricate and dynamic nature of contemporary cybercrimes. Many of its regulations fall behind the complexity and anonymity made possible by technologies like the dark web, encryption, and virtual private networks (VPNs). New types of cybercrimes are either not covered at all by the present statutory framework or are just partially covered. Additionally, the punishments for major crimes like hacking are frequently light, and many of these acts are classified as bailable, which weakens their deterrence power.

The lack of a centralized national procedure for reporting vulnerabilities or bugs, as well as the disarray in communication between different regulatory and enforcement agencies, are equally concerning. As a result, people, organizations, and infrastructure are always at risk of cyberattacks, fraud, and breaches. A thorough legal reform that goes beyond cosmetic changes and considers the multifaceted character of digital dangers in the twenty-first century is therefore urgently needed.

The need to acknowledge and protect data privacy as a basic right lies at the heart of the problem. In the digital era, safeguarding personal information is not just a technical problem; it is also a moral and constitutional one. Clear, legally binding guidelines for the collection, storage, processing, and sharing of data must be created, and citizens must have the authority to manage their digital identities. Therefore, the concepts of data reduction, purpose limitation, consent-based access, and accountability must be at the core of any future-ready legal framework.

Training, technology, and interagency cooperation are necessary to strengthen the state law enforcement apparatus. At the state level, specialized cyber units must be formed and reinforced with the help of strong collaborations with commercial cybersecurity companies and national organizations such as the CBI, CERT-In, and the I4C.

Additionally, India has to reevaluate its stance on international cooperation frameworks and global cyber rules, especially by thinking about joining the Budapest Convention on Cybercrime. By doing this, India would be able to improve its cross-border investigative skills, conform to international norms, and make it easier for information to be shared in order to successfully tackle transnational cybercrimes.

12. Suggestions

A. Growing Initiatives for Public Awareness:

Creating a technologically aware culture is one of the most important ways to combat cybercrime. Due to a lack of education and exposure to technology, rural and underdeveloped areas continue to be more vulnerable, although metropolitan inhabitants may have a modest awareness of online hazards. To start focused digital literacy initiatives, state police departments should work with non-profits, local government agencies, and educational institutions.

B. Investing in Technology and Training:

Because cybercrime is evolving so quickly, police forces must constantly increase their capabilities. Regular, organized training programs for staff members in subjects like cryptocurrency investigations, ethical hacking, cyber forensics, and AI-assisted surveillance should be a top priority for the Madhya Pradesh Police and other state agencies. It is crucial to make investments in cutting-edge machinery including forensic labs, cyber range simulators, and data recovery tools.

C. Improving International and Inter-State Cooperation:

State police forces can no longer operate in isolation due to the transnational character of cybercrime. Institutionalized structures for interstate collaboration, such as pooled cyber intelligence databases and collaborative task teams, are desperately needed. Establishing strong avenues for global cooperation is equally important, especially with organizations like Interpol, Europol, and regional cybersecurity alliances.

D. Working Together with National Organizations:

Due to the intricacy of cybercrimes, centralized technical knowledge and coordinated investigation are frequently required. Cooperation with national organizations like the "Central Bureau of Investigation (CBI)", "Indian Cyber Crime Coordination Centre (I4C)", and "CERT-In (Indian Computer Emergency Response Team)" becomes essential in high-profile or multi-jurisdictional investigations like the "Bhopal phishing scam." .

E. Accelerating Reforms in the Law:

While technology advancements are important, the legal system must also change. Cases involving cybercrime are infamously complicated and time-consuming, which delays justice and reduces deterrence. The creation of fast-track cyber courts or specific cybercrime benches inside the Indian legal system is urgently needed. Judges with training in digital law, data security, and cutting-edge technologies like blockchain, artificial intelligence, and the dark web must serve in these courts. To eliminate jurisdictional and enforcement loopholes, the Information Technology Act of 2000 must also be amended and harmonized with worldwide legal standards. In the context of social media and technology, a clear legislative roadmap that includes additional offenses, harsher fines, and clarification on intermediary accountability must be created.

F. Establishing Specialized Cybercrime Courts

Due to the exponential increase in cybercrimes, traditional courts frequently struggle to handle the intricacy and technicality of these cases. At the state and district levels, the creation of specialised cybercrime courts would guarantee the prompt and targeted resolution of cyber cases. Judges, prosecutors, and employees with sufficient education and experience in digital forensics, information technology regulations, and cyber procedural protocols ought to staff these courts.