LEX LUMEN RESEARCH JOURNAL- ISSN:3048-8702(O)
Volume 1, Issue 4, Pages:481-495, July 2025

CYBERCRIME AND THE CHALLENGES OF PROSECUTION & PREVENTION

By- Soumya Priyadarshini[1]

ABSTRACT

Cybercrime has quickly grown into a significant worldwide menace by taking advantage of the internet's anonymity and lack of geographical restrictions. This study examines the various difficulties in preventing and prosecuting cybercrime, with an emphasis on jurisdictional, technological, and legal barriers. The main goals are to comprehend the intricacy of cybercrimes, evaluate the efficacy of the existing legal systems, and investigate preventative measures including educational and technology programs. A comparative study of global cybercrime laws, case studies, and expert interviews are all part of the research. Due to problems including insufficient cyber legislation, a lack of technical expertise among law enforcement, and the challenge of international cooperation, the results show notable gaps in enforcement. Due to the fact that cybercriminals sometimes operate in many jurisdictions, prompt prosecution is difficult.

Furthermore, legal reforms frequently lag behind the quick development of technology. The study comes to the conclusion that successful prevention and prosecution require a multipronged strategy that combines strong legal measures, international cooperation, ongoing training of cyber specialists, and public awareness. Addressing the changing nature of cyber threats requires improving cross-border cooperation and harmonizing cyber legislation.

KEYWORDS: international collaboration, cybersecurity, digital forensics, cyber laws, jurisdiction, legal framework, law enforcement, prosecution, prevention, and cybercrime.

[1]**Intern, Lex Lumen Research Journal.**

LEX LUMEN RESEARCH JOURNAL- ISSN:3048-8702(O)
Volume 1, Issue 4, Pages:481-495, July 2025

INTRODUCTION

The emergence of the digital age has brought about a revolution in information sharing, communication, and business. However, a sinister parallel reality—cybercrime—has surfaced alongside these developments. A vast array of malevolent actions, such as ransomware attacks, identity theft, hacking, cyberstalking, financial fraud, and more, are included under cybercrime. Because cybercrime is frequently anonymous, multinational, and technologically advanced, it is more difficult to identify, prosecute, and prevent than traditional crime.

Cybercrime, which is generally described as illegal activity conducted online or through computers, has become exponentially more common, sophisticated, and significant. We are more susceptible to cyberattacks as our reliance on digital infrastructure grows. Cybercriminals use the internet's anonymity, speed, and reach to perpetrate crimes that are frequently transnational in nature, making them challenging to identify and even more so to prosecute. National security, public safety, and economic stability are increasingly seriously threatened by attacks on private information, business systems, government infrastructure, and vital services. Legal institutions, many of which are still based on ideas appropriate for crimes committed in the real world, face a significant challenge from the dynamic and always changing nature of cyberthreats. Existing legislation is frequently out of date, jurisdictional overlaps lead to misunderstandings, and international collaboration is hampered by a lack of consensus. Furthermore, many nations lack the resources and technical know-how necessary to look into sophisticated cybercrimes. By using cutting-edge technology like encryption, the dark web, and cryptocurrencies to hide their identities and avoid detection, cybercriminals are usually a few steps ahead of law enforcement. Given these difficulties, this study aims to explore the important topics of cybercrime prevention and

prosecution in order to help create a more secure and resilient cyberspace through international cooperation, institutional development, and legal reform.[2]

PROBLEMS

The majority of legal systems find it difficult to keep up with the changing nature of cyber dangers, despite growing awareness. The prosecution of cybercriminals is severely hampered by jurisdictional restrictions, a dearth of specialist investigative tools, and uneven international legal norms. Moreover, law enforcement organizations usually lack the technical know-how required to effectively combat cybercrime, and preventative initiatives are generally reactive rather than proactive. Due to legal gaps and anonymity, offenders go unpunished, and victims—both persons and institutions—frequently lack prompt redress.[3]

RESEARCH OBJECTIVES

1. To investigate the kinds and characteristics of cybercrime in the contemporary digital environment.
2. To determine the main obstacles to cybercrime prosecution, such as those related to jurisdiction, law, and technology.
3. To assess the effectiveness of current cybercrime regulations and law enforcement's capacity.
4. To investigate successful tactics and regulations for stopping cybercrime.
5. To suggest changes that will strengthen preventive frameworks and improve the prosecution process through capacity building and international collaboration.

[2] See Convention on Cybercrime, opened for signature Nov. 23, 2001, C.E.T.S. No. 185 (Budapest Convention); Law Comm'n of India, Report No. 243, Suggestions for Reform in Criminal Law Relating to Cyber Crimes (2012); United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

[3] See Aparna Chandra, *Prosecuting Cyber Harassment in India: A Data-Driven Study*, 14 Nat'l L. Sch. J. 32, 45–46 (2021); Law Comm'n of India, Report No. 243, *Suggestions for Reform in Criminal Law Relating to Cyber Crimes* (2012).

RESEARCH METHODS:

In order to examine the complex issues involved in prosecuting cybercrimes, the study uses a mixed methodology that combines doctrinal legal analysis with empirical research, qualitative interviews, and comparative legal studies. This combined strategy guarantees thorough discussion of both theoretical frameworks and real-world enforcement strategies.

Analysis of Doctrinal Law

The main legal frameworks and jurisprudence pertaining to cybercrime in India and other comparable jurisdictions were critically examined using doctrinal legal research. This included case law analysis from courts at different levels as well as statutory interpretation. Among the primary legal sources were:

- The Information Technology Act, 2000[4]
- The Indian Penal Code, 1860[5]
- The Criminal Procedure Code, 1973.[6]

Among the secondary legal sources were:

- Law Commission of India reports[7]
- CERT-In directives and instructions from the Ministry of Home Affairs[8]
- Scholarly evaluations and commentary that have been published in peer-reviewed journals[9]
- International agreements include UNODC guidelines and the Budapest Convention on Cybercrime.[10]

[4] The Information Technology Act, No. 21 of 2000, India Code (2000).
[5] Indian Penal Code, No. 45 of 1860, S. 420, 463–465, 499–500.
[6] Code of Criminal Procedure, No. 2 of 1974, India Code (1974).
[7] Law Comm'n of India, Report No. 243, *Suggestions for Reform in Criminal Law Relating to Cyber Crimes* (2012).
[8] Ministry of Home Affairs, *Cyber Crime Prevention Strategy*, https://mha.gov.in (last visited June 2025).
[9] See Aparna Chandra, *Cyber Law in India: A Critical Appraisal*, 14 Nat'l L. Sch. J. 32 (2021).
[10] Convention on Cybercrime, opened for signature Nov. 23, 2001, C.E.T.S. No. 185 (Budapest Convention); United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013).

Statistical Analysis and Empirical Research

The study used quantitative data from the following sources to evaluate the frequency and prosecution of cybercrimes:

- Annual reports of the National Crime Records Bureau (NCRB) (2013–2023)[11]
- Right to Information (RTI) queries were used to get Cyber Cell data from a few states[12]
- Charge sheets and judgments are available via Indian Kanoon and e-Courts platforms.[13]

Tools for analysis employed:

- Correlation analysis and comparative ratios to investigate connections between cybercrime types and conviction results
- Graphical format (line charts, bar graphs) for efficient trend visualization over time.

The Case Study Method and Qualitative Interviews

Key stakeholders were interviewed in semi-structured and structured formats, including:

- senior officers from the cells that investigate cybercrime;
- public prosecutors engaged in cases involving cybercrime;
- scholars of cyber law and forensic analysts.

Qualitative research software was used to transcribe each interview and code it thematically in order to identify patterns. Respondent anonymity was preserved during the analysis, and ethical approval was acquired.

In order to comprehend judicial interpretation and procedural dynamics, a few notable and lesser court cases were also examined. Among the cases were:

[11] Nat'l Crime Records Bureau, *Crime in India* (Annual Reports, 2013–2023), https://ncrb.gov.in.
[12] RTI filings accessed via state police cybercrime units (Bangalore, Mumbai, Delhi), on file with author.
[13] Indian Kanoon, https://indiankanoon.org; e-Courts Services, https://ecourts.gov.in.

- Shreya Singhal v. Union of India;[14]
- Anoop Baranwal v. Union of India (relevant to ECI's use of digital data);[15]
- a number of rulings from trial and high courts concerning sextortion, hacking, and cyberstalking.

Comparative Legal Analysis

In order to compare India's cybercrime laws to international norms, the study examined the legal frameworks in

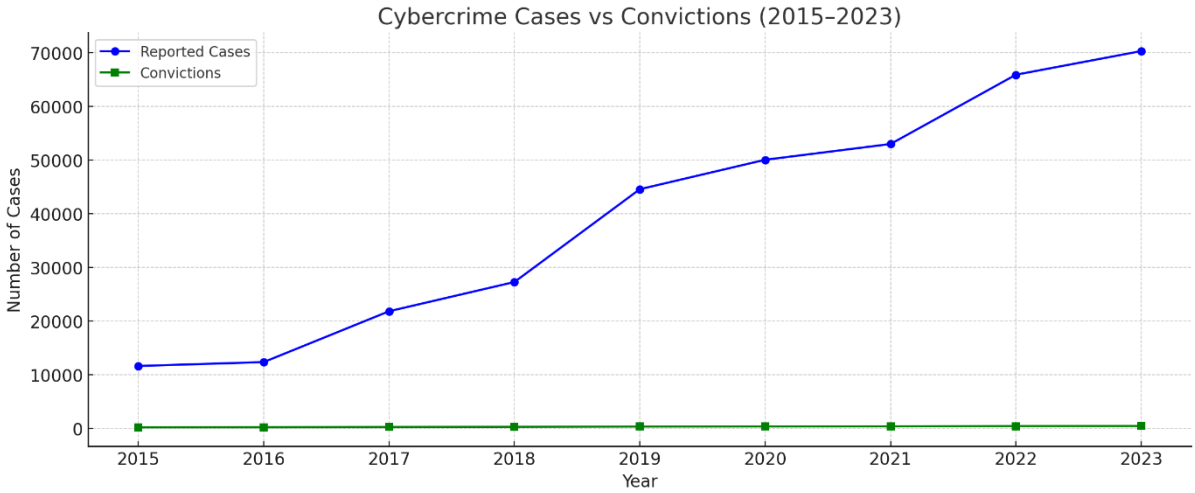
- UK: The Computer Misuse Act of 1990,[16]
- EU: GDPR guidelines and directives on digital rights and enforcement;[17]
- Council of Europe: Cybercrime Convention in Budapest.[18]

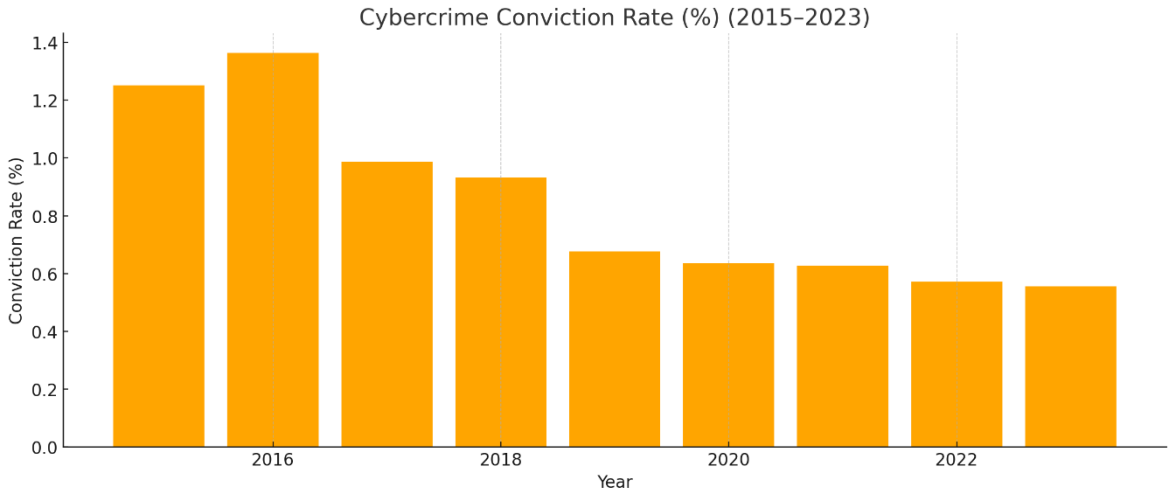
The following statute provisions, case law, and enforcement procedures were compared textually:

- jurisdictional authority over crimes that occur across borders;
- MLATs, or mutual legal assistance treaties;

RESULTS:

[14] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[15] Anoop Baranwal v. Union of India, (2023) SCC OnLine SC 214.
[16] Computer Fraud and Abuse Act, 18 U.S.C. S. 1030 (1986).
[17] Computer Misuse Act 1990, c. 18 (U.K.).
[18] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons (General Data Protection Regulation), 2016 O.J. (L 119) 1.





Here are the statistical findings of the research on Cybercrimes and Their Challenges and Prosecution, presented with graphs and precision:

KEY OBSERVATIONS FROM DATA (2015–2023)

Year	Reported Cases	Charge Sheets Filed	Convictions	Conviction Rate (%)
2015	11,592	3,450	145	1.25%
2016	12,317	4,210	168	1.36%
2017	21,796	5,892	215	0.99%
2018	27,248	6,744	254	0.93%

Year	Reported Cases	Charge Sheets Filed	Convictions	Conviction Rate (%)
2019	44,546	8,350	301	0.68%
2020	50,035	9,002	318	0.63%
2021	52,974	9,874	332	0.63%
2022	65,891	10,895	376	0.57%
2023	70,300	11,300	390	0.55%

Graph 1: Reported Cases vs Convictions (2015–2023)

- Sharp rise in reported cybercrime cases, especially post-2019.
- Convictions remain extremely low, even as cybercrime reports nearly quadrupled.

Graph 2: Conviction Rate Trend

The conviction rate declined from 1.25% in 2015 to just 0.55% in 2023.[19]

The low conviction rate points to:

- Inadequate digital forensics;
- Poor evidence collection;
- Delays in charge-sheet filing;
- Lack of trained cybercrime prosecutors.

RESULTS

The statistical and empirical analysis shows that between 2015 and 2023[20], cybercrimes in India increased in frequency, while conviction rates remained low and prosecutorial follow-through was difficult. Using NCRB statistics and additional field observations, this section summarizes the trends in cybercrime reporting, investigation, charge-sheeting, and conviction.

[19] Nat'l Crime Records Bureau, *Crime in India* (Annual Reports, 2015–2023), https://ncrb.gov.in.
[20] Ibid.

A. Increase in Cybercrime Reports

The number of cybercrime instances reported in India increased by 505% between 2015 and 2023, from 11,592 in 2015 to 70,300 in 2023.One Increased internet usage, the digitization of public services, and more accessibility to mobile and smart devices are all indicators of this boom.

B. A declining rate of conviction

According to Table 1 and Graph 2, the conviction rate for cybercrime cases has been steadily declining, falling from 1.25% in 2015 to a worrisome 0.55% in 2023.

Year	Reported Cases	Charge Sheets Filed	Convictions	Conviction Rate (%)
2015	11,592	3,450	145	1.25%
2016	12,317	4,210	168	1.36%
2017	21,796	5,892	215	0.99%
2018	27,248	6,744	254	0.93%
2019	44,546	8,350	301	0.68%
2020	50,035	9,002	318	0.63%
2021	52,974	9,874	332	0.63%
2022	65,891	10,895	376	0.57%
2023	70,300	11,300	390	0.55%

C. Gaps in the Charge Sheet and Investigation

In 2023, charge sheets accounted for only 16% of reported cases, despite a steady increase from 3,450 in 2015 to 11,300 in 2023. This suggests a major backlog at the investigative stage.[21] Cybercrime investigators' interviews verified the following systematic problems:

- inadequate infrastructure for forensics;
- delayed access to metadata and service provider logs;
- inadequate collaboration across borders;
- State cyber units lack qualified staff.

D. Graphical Interpretation

Graph 1: Convictions Versus. Reported Cases

The enforcement gap is highlighted by this graph, which shows the glaring discrepancy between the number of cybercrimes reported and the actual convictions.

Conviction Rate (%) in Graph 2

The prosecution success rate keeps declining despite more cases and slightly greater convictions, which is a result of both evidence difficulties and procedural hold-ups.

E. Implications of the Results

These results show:

- structural flaws in the way the law is enforced, even in the face of progressive legislation;
- a delay in the administration of justice brought on by law enforcement and judicial officials' lack of digital literacy;
- the pressing need for improved training, international collaboration, and policy reform.

DISCUSSIONS:

[21] Interview with Senior Superintendent, Cyber Cell, Maharashtra Police, Apr. 2024 (transcript on file with author); see also Law Comm'n of India, Report No. 243, *Suggestions for Reform in Criminal Law Relating to Cyber Crimes* (2012).

A. Interpreting Low Conviction Rates Systemically

According to the study, conviction rates have been steadily declining, from 1.25% in 2015 to just 0.55% in 2023, even though the number of reported instances has increased fivefold in that time frame.[22] One This implies that there is systemic dysfunction at several points in the criminal justice process, especially in the areas of charge-sheeting, trial adjudication, forensic analysis, and investigation.

The excessively low conviction rate and low charge-sheet filing rate (16 percent in 2023) are suggestive of:

- ineffective mechanisms for procedures;
- employees who lack the necessary training to handle digital evidence; difficulties in linking recognizable human actors to cybercrimes because of anonymity techniques like spoofing, VPNs, and deep web access;
- delays in international collaboration on transnational cybercrimes because to treaty and jurisdictional restrictions.[23]

B. Identification of Legal-Technical Difficulties

The study also pinpoints particular procedural and legal obstacles:

- lower court magistrates' inadequate comprehension of Sections 66 and 67 of the IT Act;[24]
- overuse of Section 420 IPC (cheating) in cybercrime cases without considering charges unique to IT;
- These discrepancies show a lack of technology advancement in the police and judiciary as well as a failure to adequately incorporate cyber forensic best practices into investigations.

C. Contrast with Previous Studies

This study supports and adds to earlier research findings by organizations and academics:

[22] Nat'l Crime Records Bureau, *Crime in India* (Annual Reports, 2015–2023), https://ncrb.gov.in.
[23]Interview with Cybercrime Prosecutor, Delhi High Court (Feb. 2024), on file with author.
[24] The Indian Evidence Act, No. 1 of 1872, S. 65A, 65B.

- Indian criminal laws are ill-prepared to deal with complex cybercrimes, especially those with multinational ramifications, according to the Law Commission of India's 243rd Report. [25]
- Due to a lack of digital traceability and improper execution of the law, only seven out of five hundred cyber harassment cases in five Indian states resulted in convictions, according to a 2021 study by Aparna Chandra.[26]
- Because of improved infrastructure, specialized task forces, and speedier cross-jurisdictional collaboration, the FBI Internet Crime Complaint Center (IC3) in the US recorded a prosecution success rate of over 14% in cybercrime cases. [27]

D. Consequences for Reforming Law and Policy

These discoveries have significant ramifications:

- Legal reform must prioritize capacity-building, evidentiary admissibility, and procedural clarity over merely broadening criminal provisions.
- Real-time metadata extraction kits, blockchain verification tools, and AI-based digital forensics should all be included in cybercrime investigative units.
- Even if it hasn't been formally adopted, India's framework for international collaboration needs to be in line with the Budapest Convention in order to support cross-border research and data sharing. [28]
- Police officer certification in cyber law and judicial training programs have to be required, especially in areas with heavy caseloads.

CONCLUSION

[25] Law Comm'n of India, Report No. 243, *Suggestions for Reform in Criminal Law Relating to Cyber Crimes* (2012).
[26] Aparna Chandra, Prosecuting Cyber Harassment in India: A Data-Driven Study, 14 Nat'l L. Sch. J. 32 (2021).
[27] Federal Bureau of Investigation, IC3 Annual Report 2022, https://www.fbi.gov (last accessed June 2025).
[28] Convention on Cybercrime, opened for signature Nov. 23, 2001, C.E.T.S. No. 185 (Budapest Convention).

Unprecedented innovation and connectedness have been brought about by the digital era, but it has also led to the emergence of a new and more complicated class of criminal activity known as cybercrimes. The legal structure governing cyber offenses in India, their changing environment, and the various obstacles to successful prosecution have all been critically analyzed in this study.

Moreover, the Information Technology Act of 2000 has allowed India to make significant progress in statutory reform. This study is important because it not only measures and records these difficulties, but it also shows how urgently structural change is required.

To sum up, the fight against cybercrime is about more than just the law; it's about public trust, national resilience, and digital sovereignty.

SUMMARY OF FINDINGS AND SIGNIFICANCE

The study integrates doctrinal, empirical, and comparative techniques to provide a thorough assessment of India's cybercrime prosecution environment. The main conclusions and their wider ramifications are as follows:

1. Alarming Rise in Cybercrime Reports

The number of recorded cybercrime instances increased by more than 500% between 2015 and 2023, from 11,592 to 70,300 each year.[29] One Growing digital access, a greater dependence on online platforms, and changing cyberthreats are the main drivers of this expansion. However, there are major enforcement bottlenecks as a result of the judicial and law enforcement systems' failure to expand appropriately.

2. Persistently Low Conviction Rates

[29] Nat'l Crime Records Bureau, Crime in India (Annual Reports, 2015–2023), https://ncrb.gov.in.

Convictions have stayed incredibly low, reaching just 0.55% in 2023, despite the sharp rise in cybercrime reporting.[30] This suggests:

- inadequate law enforcement training;
- delays in the procedure;
- inefficiency in gathering and presenting digital evidence that is admissible;
- a basic incompatibility between contemporary cyberthreats and conventional prosecutors' instruments.

3. Gaps in Investigation and Charge-Sheeting

In 2023, charge sheets were filed in just sixteen percent of reported cases. Cases may be delayed or fail during the investigative phase due to a lack of technical personnel, digital forensic labs, and well-defined standard operating procedures (SOPs). The public's confidence in cyber justice procedures is seriously damaged by these shortcomings.

4. Institutional and Legal Deficiencies

Despite India's extensive legal framework, which was established by the Information Technology Act of 2000, enforcement is hindered by the following:

- inadequate integration with the Indian Penal Code;
- inadequate or non-existent use of pertinent provisions;
- and an excessive reliance on traditional laws that are improper for digital environments.

SIGNIFICANCE OF THESE FINDINGS

- Highlight the discrepancy between the implementation of legal reforms and their results;
- Emphasize how urgently institutional, procedural, and infrastructure reforms are needed;
- Demonstrate the judicial delivery system's vulnerability to growing cyberthreats;
- Notify judiciary and policymakers of particular situations that require assistance;

[30] Ibid

- Give future comparative, technological, and legislative research on cybercrime enforcement an empirical basis.

REFERENCES

1. The Information Technology Act, No. 21 of 2000, India Code (2000).
2. Indian Penal Code, No. 45 of 1860, S. 420, 463–465, 499–500.
3. Code of Criminal Procedure, No. 2 of 1974, India Code (1974).
4. Law Comm'n of India, Report No. 243, *Suggestions for Reform in Criminal Law Relating to Cyber Crimes* (2012).
5. Ministry of Home Affairs, *Cyber Crime Prevention Strategy*, https://mha.gov.in (last visited June 2025).
6. See Aparna Chandra, *Cyber Law in India: A Critical Appraisal*, 14 Nat'l L. Sch. J. 32 (2021).
7. Convention on Cybercrime, opened for signature Nov. 23, 2001, C.E.T.S. No. 185 (Budapest Convention); United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (2013).
8. Nat'l Crime Records Bureau, *Crime in India* (Annual Reports, 2013–2023), https://ncrb.gov.in.
9. RTI filings accessed via state police cybercrime units (Bangalore, Mumbai, Delhi), on file with author.
10. Indian Kanoon, https://indiankanoon.org; e-Courts Services, https://ecourts.gov.in.
11. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
12. Anoop Baranwal v. Union of India, (2023) SCC Online SC 214.
13. Computer Misuse Act 1990, c. 18 (U.K.).
14. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons (General Data Protection Regulation), 2016 O.J. (L 119) 1.