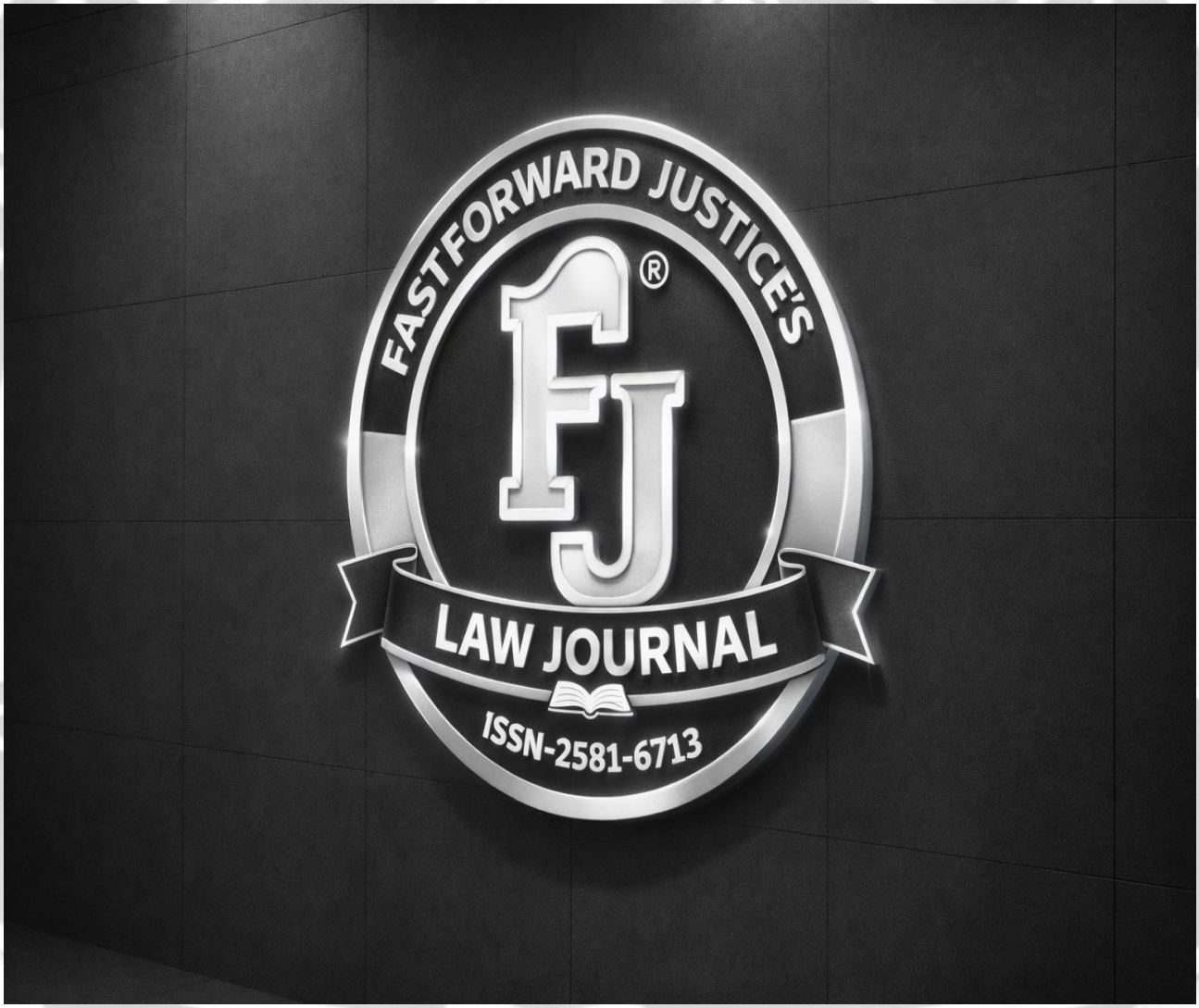
FastForward Justice's Law Journal (e-ISSN: 2581-6713)
Volume VI Issue II (March–April 2026)

Policing The Digital Frontier: Prosecuting Cybercrimes And Online Scams In India Authored by : Aaron George Biju Available at Link



Scan this below barcode to verify the plagiarism authenticity of this Published Paper

FastForward Justice's Law Journal (e-ISSN: 2581-6713)
Volume VI Issue II (March–April 2026)

CLICK HERE TO READ DISCLAIMER

CLICK HERE TO SEE EDITORIAL BOARD

CLICK HERE TO SEE PUBLISHER DETAILS

ABSTRACT

Online frauds and cybercrime have been drastically rising due to the high rate of conversion of India to digital economy that has transformed the character of crime. The widespread adoption of online payment systems, e-commerce, and social networking websites has enlarged the attack area of cybercriminals who engage in ransomware attacks, Internet fraud, identity theft, impersonation, cryptocurrency fraud and breach of data. By official estimates, over the last decade, cybercrime complaints and monetary losses have grown exponentially posing significant challenges to law enforcement and the criminal justice system. The Information Technology Act of 2000 and Bharatiya Nyaya Sanhita of 2023, procedural rules pertaining to electronic evidence, and the institutional role of cyber police agencies, CERT-In, and central coordination agencies are all examined critically in this essay. The research evaluates the effectiveness of cybercriminal prosecution in India based on the doctrine of law with the support of judicial precedents, enforcement trends, and cross-country perspectives of countries such as Singapore, the United States, and the United Kingdom. The study concludes that with good legal framework in place, India has successfully developed a comprehensive and dynamic legal framework, but the lack of jurisdiction, inadequacy in investigative capability, low conviction rates, procedural challenges and interagency and international collaboration, alongside a shift to proactive and technology-focused enforcement remains the limiting factors associated with enforcing the digital frontier. It concludes that cybercrime will still outmatch the prosecutorial powers of India unless it makes systemic changes to increase trust in the digital ecosystem.

Keywords: Cybercrime, Online Scams, Information Technology Act, Digital Policing, Cyber Law, India

LITERATURE REVIEW

Over the past few years, the topic of cybercrime and online frauds has attracted growing academic attention amid the rapidly digitalized governance institutions and the economies. The primary issues of the early legal research conducted with regard to cybercrime in India were the sufficiency and extent of the Information Technology Act, 2000. The IT act is the first law in India to respond to cybercrimes, and researchers such as S.K. Verma examined the punitive clauses and area of jurisdiction of the law. These reports demonstrated that, despite the fact that the Act provided significant categories of crimes, such as identity theft, hacking and computer-related fraud, it was largely reactive and technology-focused and that it was necessary to revise the Act on a regular basis to address emerging cyber threats.

Another important body of literature is the technological and criminological nature of cybercrime, which is upheld by this corpus of material by the Supreme Court was that the judicial approach in cybercrime cases should be to rely on the provisions of the IT Act, as well as the normal criminal law. Susan W. Brenner suggests that cybercrime is a structural threat enabled by automation, global connectedness and anonymity. In an analogous manner, Nir Kshetri will concentrate on the online fraud as a global economy, signifying that there are organized structures and financial incentives behind online fraud. These publications are useful in explaining why it is difficult to fight cybercrime with traditional methods of law enforcement and why there is still low prosecution rates despite a rise in complaints. Legal research also discussed judicial and evidentiary challenges in a detailed manner.

Several authors have discussed the high requirements of an acceptance of electronic evidence under Section 65B of the Indian Evidence Act following some of the landmark Supreme Court decisions such as Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Government papers and policy-oriented research form a major part of the literature as their

rules are considered to pose a barrier to effective prosecution due to lack of technical background of investigators. In policy reviews, governmental and non-governmental agencies consider the factual data provided in the reports published by the National Crime Records Bureau (NCRB) regarding the increasing nature of cybercrime in India, particularly online financial crimes. These studies emphasize the unavailability of specialized judicial instruments and state inequality in competence in the context of cybercrime enforcement in nations such as Singapore, the United States and the United Kingdom. To enhance the outcomes of prosecution, scholars call on the need to have intelligence-led policing, specialist cybercrime teams, and well-developed international cooperation on top of legal sufficiency.

Altogether, the literature currently available provides valuable information regarding the legal framework, technological challenges, and legal strategies of combating cybercrimes. Much of this work is, however, still scattered and has focused either on statutory requirements or has used a criminological or technological prism without regard to the outcomes of enforcement and the effectiveness of prosecution.

RESEARCH GAP

The literature on cybercrime and online scams still has some serious gaps, particularly concerning the Indian environment. To begin with, much of the prevailing legal research focuses on the substantive terms of the Information Technology Act of 2000 without a sufficient examination of their operation in real-life investigations and prosecution. There is a lack of empirical analysis of statutory frameworks and actual outcomes of enforcement, which include conviction rates, delays and failures in procedures. Second, there has been a lack of a combined study that connects evidentiary jurisprudence and institutional potential, as the opinions of the courts on the use of electronic evidence have been widely discussed.

Section 65B compliance is now criticized in isolation in the available material but fails to adequately discuss how best practices in other nations can be adapted to Indian federal system, resources, and volume of cybercrimes. There has been no research to put comparative models within the institutional and legal provisions in India. Third, instead of the effectiveness of prosecution, most of the policy reports focus on cybercrime awareness and prevention. Finally, the literature that is currently in publication will not often deal with victim-centric results, such as restitution of financial loss and deterrence through prompt adjudication, in an effort to offer a comprehensive methodology to the reader. This fragmentation denies the ability to come up with comprehensive reform responses to cybercrime prosecution.

Through a thorough analysis of the structure of cybercrime prosecution in India, the work is expected to address these deficiencies. It also considers statutory provisions, institutional procedures, enforcement statistics and judicial patterns together in order to propose context-sensitive reforms. The research is aimed at contributing to the discussion of policing the digital frontier of India by focusing on the effectiveness of prosecution and not only on the competence of legislation.

INTRODUCTION

The rapid digitalization in India has transformed day-to-day socialization, business and the government. The efforts to provide digital access, such as Digital India, Aadhaar-based identification, Unified Payments Interface (UPI), and extensive smartphone use, have significantly enhanced the digital access. By the beginning of the 2020s, India has reached the level of one of the largest internet users in the world. But cybercrime and internet fraud have thrived due to this electronic expansion, and cyber security and online policing are extremely important issues of governance. Unlike physical crimes, cybercrimes are

anonymous, transnational, technologically sophisticated and can have a profound damage without much physical presence. Online frauds that have made victims lose their money and suffer psychological trauma include phishing emails, fake calls made by customer care agents, investment fraud, romance scams, and SIM-swapping attacks. Cybercrime is a form of crime in India, which, according to the National Crime Records Bureau (NCRB), is growing at the most rapid pace.[1] The legal response to cybercrime in India is primarily based on the Information Technology Act, 2000 (IT Act) that was enacted to provide legal recognition to electronic transactions and punish cyber offenses. The conviction rates remain skewed in spite of the increased reporting regarding the issue, and this fact can be attributed to the ineffectiveness of the investigation and prosecution. The IT Act is supplemented by the Bharatiya Nyaya Sanhita, 2023's general criminal law provisions and the Bharatiya Nagarik Suraksha Sanhita, 2023's procedural protection.

Moreover, the Indian Evidence Act of 1872 regulates the evidentiary disputes that are related to the electronic documents. The gap between the presence of cyber laws and their effective implementation is a common point that we find in the scholarly literature. The authors such as Susan Brenner and Kshetri believe that cybercrime thrives in the regions where the law is failing to keep pace with the technical innovations.[2] Another issue that is highlighted by Indian scholars is the absence of inter-agency cooperation, misused procedures, and inadequate digital forensics experience that negatively affect prosecutions of cybercrimes. The decisions made by the courts also indicate that cases often lose due to the violation of procedure and evidence and not due to a deficiency of the criminal motive.

[1] *National Crime Records Bureau, Crime in India 2022 (Gov't of India 2023).*
[2] *SUSAN W. BRENNER, CYBERCRIME: CRIMINAL THREATS FROM CYBERSPACE 98–102 (Praeger 2010).*

With this in mind, this paper examines the institutional capacity, legal framework, enforcement outcomes, and similar international practice trends in an attempt to explore how India approaches policing of cybercrime and online scams.

LEGAL AND INSTITUTIONAL FRAMEWORK

The prosecution of the cybercrime and online frauds in India is regulated by a multi-layered legal and institutional framework comprising the special cyber legislation, the general criminal law, the procedural protection provisions, the evidence provisions, and the administrative institutions. This model is an attempt of India to change traditional criminal justice systems to the requirements of the anonymous, borderless, and technologically driven criminal activity. Nevertheless, scope of its legal provisions is equally important to the effectiveness of this framework compared to institutional coordination, investigative capability and judicial interpretation. India has a policy on cybercrime that is based on the Information Technology Act, 2000 (IT Act). The Act was enacted to offer legal validity to digital signatures and e-documents. It had also criminal provisions to address computer networks and systems offenses. Section 43 of the Act obligates civil responsibility in case of unauthorized access, data damage, introduction of viruses, and interruption of computer systems. Section 66C and 66D of the Act directly cover identity-related cybercrimes on a case-by-case basis when it was performed, unintentionally, or even accidentally.[3]

The use of passwords, electronic signatures, and unique identifying features, among others, is taboo in Identity theft, which is an illegal act in Section 66C. Section 66D on cheating through personation using computer resources is one of the most common clauses used whenever dealing with cases of phishing schemes, false pretences in the guise of customer services and online impersonation. These provisions recognize that so often fraud through

[3] *Information Technology Act, 2000, §§ 66C–66D (India).*

identity is the foundation of deceit in cyberspace as opposed to in-person contact, like it is in Section 66F which defines and punishes cyberterrorism, that concerns more serious cybercrimes. This article criminalizes any acts that are directed to threaten the security, integrity, or sovereignty of India, by obtaining unauthorized access to important information infrastructure, with national security interests. Section 66F prosecutions are relatively rare but the recognition of the strategic hazards of cyber threats by the legislature is reflected by the fact that it is included. The IT Act establishes regulatory bodies alongside criminal provisions. Section 70B established the Indian Computer Emergency Response Team (CERT-In) which is responsible of incident response, coordination of cyber security, and issuing advisory.[4]

The Indian system of combating cybercrime is fragmented even though the technical reviews and reports presented by the CERT-In in many cases form a substantial influence on the investigation and prosecution of law enforcement agencies. The cybercrime cells and cyber police stations that are run by state police forces are primarily in charge. The states are quite varied because of infrastructure, training and capacity and this leads to various enforcement outcomes. To solve the problem of coordination, the central government created the Indian Cyber Crime Coordination Centre (I4C) that functions as a nodal institution of information sharing and training, as well as the development of national cybercrime databases. As the technological heart of the Indian cyber security response, CERT-In coordinates the response to cyber incidents and provides the advisory. The lack of direct enforcement authorities results in the absence of effective prosecution that is based on smooth communication between CERT-In and police authorities, financial institutions, and digital intermediaries.

[4] *Information Technology Act, 2000, § 70B (India).*

In some instances of cybercrimes, there are financial intermediaries, servers, victims, and offenders who are located in different states or countries. This minimizes deterrence, complicates investigations and postpones mutual legal assistance. The lack of special cybercrime courts also contributes to delays as the general criminal courts may lack the technical skills to use complex digital evidence. India has a wide-ranging legal and administrative system to prosecute cybercrime, but it is not enforced uniformly. Even though the courts have set up very high standards of evidence and statutes have defined a wide array of cybercrimes, institutional fracturing, talent curses, and procedural mazes restrict enforcement. Thus, continuous investment in institutional capacity, specialization, and coordination is equally significant to the achievement of cybercrime prosecution as to sufficient legislation.

IMPACT ANALYSIS: LEGAL AND QUANTITATIVE EVALUATION

The effectiveness of the cybercriming prosecution system in India should be assessed both through the quantitative enforcing statistics and the qualitative judicial assessment. However, in India cybercrimes have been reported at an exponent rate in the past decade particularly in terms of identity theft, impersonation schemes, and online financial fraud. One of the categories of crime is the cybercrime that is growing the fastest in the country, as the statistics published by the National Crime Records Bureau (NCRB) indicate.[5] The prosecution outcomes are not favorable despite the drastic increase in the reports regarding online frauds with digital payment schemes, phishing websites, and fake investment opportunities as well as fraudulent customer support calls. Compared to the rate of complaints, the rate of cases resulting in charge sheets and conviction is too low. Such imbalance is evidence of structural

[5] *National Crime Records Bureau, Crime in India 2022 (Gov't of India 2023).*

imperfections in the capacity to carry out the investigations, collect evidence, and prosecute cases.

One of the important aspects is the technical advancedness of cybercrimes. Unlike the conventional crimes, cybercrimes require following the digital footprint, reviewing electronic logs, and cooperation with the platform providers, financial intermediaries, and internet service providers. The frequency of loss or corruption of electronic evidence due to delays in accessing such evidence compromises the case of prosecution and is reflected in court decisions. Courts in cybercrime proceedings have always emphasized that there must be a strict compliance with the evidentiary requirements. In the case of Anvar P.V. v. P.K. Basheer the Supreme Court stated that electronic documents can be only admitted in accordance to Section 65B of the Indian Evidence Act as long as they are provided with a legitimate certificate.[6] In Arjun Panditrao Khotkar v. The Court reiterated this position when Kailash Kushanrao Gorantyal stated that the procedural compliance cannot be waived at the cost of obtaining convictions.[7] These decisions have bolstered due process and have also resulted in acquittal in cases where investigative agencies failed to follow technical norms.

Another significant challenge is jurisdiction. Cybercrimes often have multiple jurisdictions with victims, offenders, servers and financial intermediaries being located in numerous states or countries. This complicates the investigation and delays the prosecution. The deterrent effect of the enforcement is reduced by the time-consuming nature of mutual legal aid procedures of international cybercrime. These challenges have been embraced by the courts although they explained that more institutional collaboration is required, in the numbers aspect, enforcement is still reactive and not proactive. Rather than taking an active intelligence-led policing approach, law enforcement is often taken after victims have incurred

[6] *Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).*
[7] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).*

a monetary loss. Examples of these initiatives which have demonstrated improvement, though differentially in impacts across states, include the national cybercrime reporting system and increased funding to cyber forensic laboratories. Due to this, the cybercriminals keep exploiting the loopholes in the enforcement, and prosecution of cybercrime in India is usually a futile exercise.

REFORM VIEWPOINT AND COMPARITIVE EVALUATION

The comparison of the different countries system of cybercrime implementation offers some very useful data on the possible areas of reform in India. Federal coordination, expert cybercrime divisions, and close interactions among law enforcing agencies and non-governmental organizations are some of the features of cybercrime prosecution in the United States. To manage to investigate and prosecute more complex digital crimes, specialized cybercrime prosecutors, who are technologically competent, are employed by organizations, among others, including the Department of Justice and the Federal Bureau of Investigation (FBI). The United Kingdom also adopts a more centralized and intelligence-led approach through the international cooperation treaties and the channels of whistleblowing. The U.K. approach puts a lot of emphasis on prioritization of cyber threats based on the risk, early detection and intelligence sharing. The U.K. courts have also been flexible in managing digital evidence because of striking a balance between the procedural protection and practical considerations. Singapore provides another viable example. It has an extremely well-structured cybercrime system that incorporates stringent cyber regulations with rapid investigation and criminal charges. This is due to high conviction rates that are achieved through competent detectives and special cybercrime courts, which enhances deterrence. Punishment comes immediately after detection due to the insistence on immediate

adjudication thereby enhancing compliance. According to these models, there are several reform initiatives that would be relevant to India.

First, special cybercrime benches or courts should be established that may significantly enhance effectiveness in adjudication. Such specialization would reduce delays and enhance acquaintance with technical evidence in the courts. Second, it would be feasible with an initiative toward risk-based and intelligence-led policing, which involves data analytics to identify fraud patterns and habitual offenders. Third, there would be a need to collaborate internationally more. Cybercrime being by nature international in nature, there must be immediate access to information stored abroad in order to have effective prosecution. The capabilities of the country in terms of enforcement would be enhanced through the participation in bilateral cybercrime cooperation agreements and the facilitation of mutual legal aid procedures. Fourth, investigators and prosecutors need to receive continuous education in digital forensics and cyber law to bridge the disparity between the law and practice.

Finally, a victim-centric approach in which it is possible to recover the financial loss and guarantee quick redress would help to boost the trust of the population in the cybercrime enforcement system. Based on the experience of comparison, the results of clear enforcement are important to deter cybercriminals and restore faith in digital systems.

CONCLUSION

Cybercrime and online scams are one of the largest problems of the rapidly developing online economy of India. The general criminal law, Information Technology Act of 2000 and

procedural protections have all helped the country in establishing a holistic statutory framework, but the effectiveness of enforcement remains uneven. Courts are vulnerable to institutional and procedural incompetency, and quantitative evidence indicates that the cybercrime regime in India has a worrying disproportion between reported cases of cybercrime and successful convictions and prosecutions. The analysis reveals that major challenges of the Indian cybercrime regime are institutional capacity, investigative prowess, jurisdictional complexity, and compliance with procedures, instead of insufficient legislation. Specialization, aggressive policing, and global cooperation are the key elements in effective cyber policing, which India should adopt with comparative perspective of such nations as Singapore, United States, and the United Kingdom. This would need investments in digital forensic infrastructure, the formation of special cybercrime courts, continuous capacity building of the law enforcement agencies as well as strengthening international contact points. Without such measures, law enforcement will not be able to keep pace with cybercrime and undermine trust in digital governance and compromise personal and financial security. This is why an efficient and flexible system of cybercrime prosecution is vital to the police and to the confidence in the Indian cyberspace.