A Comprehensive Examination of the Cybercrime Indian Judiciary and Legal System

Subal Chakravarty[1], Dr. Bimal Kumar Baishya[2]
[1]*Research Scholar Mahapurusha Srimanta Sankaradeva Viswavidyalaya*
[2]*Professor cum Research Supervisor Mahapurusha Srimanta Sankaradeva Viswavidyalaya*

***Abstract*—A complete examination of cybercrime in India involves numerous facets, including the type of criminals and the emerging legal jurisprudence linked to such crimes. Cybercrime is defined as criminal activity undertaken over the internet or via digital methods, and it has been on the increase owing to the increasing dependence on technology in daily life. Cybercriminals come in a variety of forms, from inexperienced hackers looking for fame to organized crime groups using sophisticated methods to get money. This section explores the traits of these criminals, their intentions, and the ways in which they take advantage of weaknesses in digital systems. Judicial jurisprudence in India has been changing to handle the issues provided by cybercrime. The legal structure concerning cybercrimes is mainly influenced by the Information Technology Act of 2000, combined with several modifications and other relevant acts. Courts have started to construct precedents that interpret the applicability of existing laws to cybercrime, considering both the intricacies of technology and the necessity for justice in situations involving digital misdeeds. Examining case studies that showcase important rulings and how they represent the judiciary's stance on cybercrime is an important part of this examination. These instances clarify the burden of evidence, the concepts of culpability, and the difficulties in prosecuting cybercriminals. The paper highlights the importance for continual law change and public awareness to tackle cybercrime successfully. As technology continues to change, so too must the laws and judicial knowledge around these acts, ensuring that justice is delivered and that victims are supported in their quest of restitution.**

***Index Terms*—cybercrime, digital, judicial, criminals, IT Act**

I. INTRODUCTION

The fast spread of digital technology in India has drastically impacted the criminal scene, leading to a collision between conventional legal frameworks and current technical difficulties. With more than 800 million people using the internet, cyber-enabled crime is flourishing in India, where individual hacking incidences have given way to a sophisticated, well-organized, international network. This extensive analysis digs into the present condition of cybercrime in India, evaluating data from the National Crime Records Bureau (NCRB) that suggests a large growth in such crimes. It also traces the development of legal frameworks from the Indian Penal Code (IPC) to the Bharatiya Nyaya Sanhita (BNS), highlighting the shifting characteristics of offenders, particularly from areas like Jamtara to Mewat. In the light of advances in artificial intelligence, it also examines intricate judicial interpretations of electronic evidence, intermediary responsibility, and individual rights. In India, the connection between technology and law is constantly changing as criminal groups use technologies like bitcoin, deepfakes, and encryption to hide their operations. This dynamic has prompted the Indian court and legislature to evaluate and change core legal foundations. The shift to the BNS indicates an essential attempt to establish these new legal interpretations, however enforcement issues are becoming obvious. In order to provide an accurate perspective of this developing area of cybercrime in India, the publication incorporates statistics data, case law, and legislative texts.

1.1 Regional Inequalities and the Urban Challenge

The spatial spread of cybercrime shows a clustering of incidents in urban areas, which act as the economic centers of the country. In 2023, the 19 leading metropolitan cities registered 33,955 cybercrime cases, representing a considerable share of the national figure. This high concentration is due to the greater volume of digital transactions, smartphone usage, and disposable income in urban regions, which make their

inhabitants attractive targets for scammers.[1] Bengaluru, frequently regarded as India's tech hub, consistently shows elevated detection figures, which indicate both significant victimization and potentially improved reporting systems relative to other areas. In Karnataka, the financial damage due to cybercrime soared to an alarming ₹2,396 crore in 2024, marking a five-fold rise from ₹113 crore in 2022. However, the recovery rate is dismal, with merely about 9% (₹226 crore) of the embezzled money retrieved in 2024. This gap between loss and recovery highlights the efficiency disparity in investigations, where the rapid transfer of assets via cryptocurrency and mule accounts frequently surpasses the slow bureaucratic process of freezing orders.[2]

Despite the alarming statistics from the National Crime Records Bureau (NCRB), many experts suggest that these figures represent merely the "tip of the iceberg" concerning cybercrime in society. A substantial portion of cybercrimes remains underreported, primarily due to factors such as minimal financial losses associated with individual incidents (termed micro-frauds), the societal stigma attached to being a victim, particularly in cases of sextortion and matrimonial fraud, and the challenges involved in filing First Information Reports (FIRs). The prevalent focus on financial fraud tends to obscure the pervasive incidence of non-financial issues, which include cyberstalking, doxxing, and online harassment, issues that disproportionately affect women and children. Furthermore, the statistics from 2023 indicate a troubling rise in attacks against vulnerable populations, highlighted by a significant 28.8% surge in crimes against Scheduled Tribes (ST) during the year.[3]

II. OBJECTIVE OF THE STUDY

The paper discusses the Indian judiciary's structure and function, emphasizing its role in ensuring justice amid technological advancements. It examines cybercrime legislation, highlighting existing loopholes and the need for amendments to address digital offenses. The study combines legal and socio-political research to assess the socio-economic impacts of criminal elements exploiting cyber vulnerabilities and advocates for enhanced collaboration between the legal and tech sectors to create effective frameworks for combating cybercrime while complying with international standards and protecting individual rights.

III. RESEARCH METHODOLOGY

Research is defined as a systematic investigation into a subject, involving a methodology that encompasses the various steps taken by the researcher and the rationale for these steps. A firm grasp of the research problem is necessary for effective research. The current study is of a doctrinal nature, employing literature surveys and documentary analysis as its research methods. In crafting this research paper, the researcher utilized a range of sources, including books, journals, and various websites.

IV. STRUCTURE OF LEGISLATION

4.1 From Colonial Laws to Digital Regulations

The legal system regulating cybercrime in India is presently undergoing changes, shifting from the colonial-era Indian Penal Code (IPC), 1860, to the recently passed Bharatiya Nyaya Sanhita (BNS), 2023. This shift is supported by the Information Technology (IT) Act, 2000, along with the Digital Personal Data Protection (DPDP) Act, 2023.

4.2 Modernization of Structure in the Bharatiya Nyaya Sanhita (BNS)

The BNS was developed to decolonize and modernize India's criminal laws. In the realm of cybercrime, it adds specific prohibitions that were noticeably lacking or vaguely stated in the IPC.

[1] *NCRB Report 2023: India Crime Statistics Explained*. (2023b). Finology.in; Finology. https://blog.finology.in/Legal-news/ncrb-report-2023

[2] TNN. (2025, April 22). *Only 9% of Rs 2,400 crore stolen by cybercriminals in Karnataka recovered in 2024*. The Times of India; Times of India. https://timesofindia.indiatimes.com/city/bengaluru/only-9-of-rs-2400-crore-stolen-by-cybercriminals-in-karnataka-recovered-in-2024/articleshow/120528765.cms

[3] zahid maniyar. (2025, November 5). *Cybercrime and the Crisis of Digital Justice: India's invisible victims online*. CJP. https://cjp.org.in/cybercrime-and-the-crisis-of-digital-justice-indias-invisible-victims-online/

- Organized Crime Institutionalization (Section 111)

In order to combat syndicates, law enforcement authorities relied on several state-level statutes like as the Maharashtra Control of Organized Crime Act (MCOCA) since the IPC lacked a common definition of "organized crime." In order to address this, the BNS introduced Section 111, which offers a thorough description of organized crime. Importantly, "cyber-crimes" are specifically included in the section's scope. Section 111 defines organized crime as any continued criminal conduct including "economic offences" and "cyber-crimes" perpetrated by persons working separately or jointly as members of an organized crime syndicate.7 This is a significant weapon against the "Mewat" and "Jamtara" gangs. Members of these gangs were previously charged with individual charges of cheating, which carried lighter terms and made bail easier. Under Section 111, the mere act of being part of a syndicate engaging in cybercrime is a distinct offence punishable by rigorous imprisonment of not less than five years, extending to life imprisonment if the crime results in the death of any person (a relevant provision given the suicides resulting from sextortion).[4]

- Reconceptualizing Cheating: Shifting from 420 to 318

"Section 420" of the IPC, commonly known as the term for cheating, has been substituted with Section 318(4) of the BNS. Although the fundamental elements of the crime—trickery and wrongful persuasion to transfer property—are largely unchanged, the BNS clause is intended to be understood alongside the updated descriptions of "digital evidence" and "electronic records" provided in the Bharatiya Sakshya Adhiniyam (BSA).[5] The highest penalty for cheating under Section 318(4) continues to be imprisonment for a period of up to seven years, along with a monetary fine. Nevertheless, the BNS focuses more on the economic effects of the offense. Legal experts contend that although the section numbers have altered, the core issue persists: the "non-bailable" aspect of the offence, frequently resulting in extended pre-trial detention for accused persons, even in cases of commercial conflicts cloaked as cyber-fraud.[6]

The Information Technology Act of 2000: The Foundation

The Information Technology (IT) Act acts as the primary law dealing with technology-related crimes in India, remaining significant even years after it was established. Significantly, it offers definitions and structures that enable the state to oversee internet operations efficiently. Essential elements consist of the Section 66 series, addressing computer-related offenses, where Section 66C (concerning identity theft) and Section 66D (related to impersonation fraud) are frequently utilized in phishing and deepfake incidents. Moreover, Section 69A provides the government with the power to restrict public access to information considered harmful to India's sovereignty and integrity, placing this section at the center of debates on internet censorship and national security. A notable element of the IT Act is the historically disputed Section 66A. This clause aimed to make "offensive" online expression a crime but was ruled unconstitutional by the Supreme Court in the significant case of Shreya Singhal v. Union of India in 2015, owing to its ambiguity. Notwithstanding this ruling, law enforcement persisted in using Section 66A for years, resulting in its designation as a "legal zombie." Additional judicial action was required in PUCL v. Union of India (2019)[7] to mandate the cessation of pending cases, highlighting a significant disparity between judicial orders and actual enforcement on the ground.[8]

---

[4] *BNS Section 111 - Organised crime.* (2024). A Lawyers Reference. https://devgan.in/bns/section/111/

[5] *Cheating & Fraud Cases – Expert Legal Help Under Section 420 IPC*. (2023). Chamberofmayank.com. https://www.chamberofmayank.com/services/cheating

[6] lawyerneeraj. (2025, July 15). *Cheating ; BNS and IPC : Section 318(4) BNS and IPC Section 420*. Advocateneerajtnarendran.info; Blogger. https://www.advocateneerajtnarendran.info/2025/07/cheating-bns-and-ipc420-bns-318.html

[7] Writ Petition (Civil) No. 1031 of 2019

[8] Johnson, H. (2019, February 27). *Revisiting Section 66A: An Afterword To A Concluded Tale - Global Freedom of Expression*. Global Freedom of Expression. https://globalfreedomofexpression.columbia.edu/updates/2019/02/revisiting-section-66a-an-afterword-to-a-concluded-tale/

4.4 The Digital Personal Data Protection (DPDP) Act, 2023

The DPDP Act changes the emphasis from punishing offenders to making data custodians responsible. It requires "Data Fiduciaries" to establish adequate security measures. Neglecting to comply can lead to a data breach, incurring fines as high as ₹250 crore.[9]

V. CATEGORIES OF CYBERCRIMINALS

5.1 The Commercialization of Deception

The profile of Indian cybercriminals has significantly evolved, transitioning from isolated hackers operating in secrecy to a burgeoning industry that supports local economies and has developed into sophisticated transnational syndicates. Jamtara in Jharkhand was historically known for its phishing scams; however, heightened law enforcement pressure has led these operations to relocate to the Mewat region, which includes Nuh district in Haryana and parts of Rajasthan and Uttar Pradesh. Sociologically, the shift can be attributed to Mewat's strategic location near the National Capital Region (NCR), providing quick access to high-speed internet and a substantial number of affluent targets in urban centers like Delhi, Gurugram, and Noida. Additionally, the geography of Mewat complicates law enforcement efforts, as perpetrators can easily evade capture by crossing state lines between Haryana and Rajasthan, exploiting the disjointed nature of police jurisdiction.

The criminal methodology in Mewat has adapted beyond the traditional "KYC expiry" scams prevalent in Jamtara, now focusing on a technique known as "Sextortion."[10] This process is executed on an industrial scale and includes several key steps:

- Luring: Criminals create fake social media accounts masquerading as attractive women to befriend potential victims.
- Engagement: Victims are coaxed into video calls on WhatsApp.
- The Trap: During these calls, either a pre-recorded obscene video is displayed or a female accomplice engages in provocative acts, prompting the victim to respond in kind.
- Extortion: These interactions are screen-recorded, after which victims are contacted by individuals impersonating police officers who threaten to release the incriminating video unless a ransom is paid.

In response to this alarming rise in cybercrime, recent initiatives like "Operation Anti-Virus" in Rajasthan have adopted rigorous strategies, including the demolition of properties linked to cybercriminals, arguing that these were funded by criminal activities.[11]

5.2 The "Digital Arrest" Trend

In 2023-2024, a novel form of fraud called "Digital Arrest" has surfaced, exploiting people's anxieties regarding governmental power. Scammers impersonating officials from the CBI, Narcotics Control Bureau (NCB), or Customs reach out to victims via video calls, utilizing backgrounds that resemble police stations. They claim that victims possess parcels loaded with drugs or are engaged in money laundering activities. The fraudsters tell the victims they are under "digital arrest," necessitating that they keep their cameras on for constant monitoring and cutting them off from family and legal counsel. Psychological manipulation strategies are used to force victims into moving their funds to alleged "confidential monitoring accounts" for supposed validation. A significant event featured the Chairman of the Vardhman Group, who was cheated out of ₹7 crore. The Ministry of Home Affairs has released advisories stating that "Digital Arrest" has no legal basis, highlighting that proper interrogations are not carried out through platforms such as Skype.[12]

[9] DLA Piper. (2024). *Data Protection Laws in India - Data Protection Laws of the World*. Dlapiperdataprotection.com. https://www.dlapiperdataprotection.com/?t=law&c=IN

[10] Tewari, S. (2022, August 21). Sextortion: how tech savvy criminals are blackmailing victims online. The Hindu. https://www.thehindu.com/news/cities/Delhi/sextortion-rackets-rose-during-pandemic/article65794981.ece

[11] Nuh cyber police nabs six people linked to interstate cybercrime network | TaxTMI. (2025). TaxTMI. https://www.taxtmi.com/news?id=59917

[12] ET Online. (2024, October 30). Digital arrest: Beware of the new cyber scam that alleges you of serious crime to extort money. The Economic Times; Economic Times. https://economictimes.indiatimes.com/news/india/dig

5.3 Chinese Lending Applications and Cross-Border Money Laundering

The "Chinese Loan App" crisis illustrates the intersection of cybercrime and predatory lending, where these apps prey on financially vulnerable individuals by offering instant micro-loans. Upon installation, users are compelled to grant access to their contacts and photo galleries. In cases of delayed repayment, which can be as minor as a day, recovery agents retaliate by accessing the victim's contacts and disseminating morphed nude images to their family, friends, and employers, a tactic that has tragically resulted in numerous suicides. Furthermore, the Enforcement Directorate (ED) has uncovered a transnational money laundering operation linked to these apps. The illicit profits are funneled through shell companies run by Indian nationals and converted into cryptocurrency or sent abroad via remittance firms, such as Nium India Pvt. Ltd. In November 2024, the ED made significant arrests of Chinese nationals in Tamil Nadu connected to the operation of these loan apps and seized assets worth crores.[13]

VI. JUDICIAL DOCTRINE ANALYZING THE CODE

The Indian judiciary plays a crucial role in the interpretation of cyber law, frequently addressing gaps in legislation and rectifying instances of executive overreach.

(1) Acceptance of Digital Evidence (Section 65B)

The key procedural issue in cybercrime trials revolves around the admissibility of digital evidence. Due to the potential for easy manipulation of digital data, legal standards necessitate stringent proof of authenticity to ensure that such evidence is reliable and valid in court proceedings.

- In the case of State (NCT of Delhi) v. Navjot Sandhu[14] (2005), the Supreme Court faced a contentious issue regarding the admissibility of electronic evidence in court. The ruling permitted the admission of such evidence without requiring a specific certificate, categorizing it as secondary documentary evidence. This decision drew significant criticism for overlooking the necessary safeguards outlined in Section 65B of the Indian Evidence Act, which governs the admissibility of electronic records and emphasizes the need for proper certification to ensure their reliability and authenticity.
- The Supreme Court case Anvar P.V. v. P.K. Basheer (2014) involved a significant ruling by a three-judge bench, which overruled a previous decision set in Navjot Sandhu. The Court established that obtaining a certificate in accordance with Section 65B(4) is a prerequisite for the admissibility of electronic records in court. This certificate serves to verify that the computer functioned correctly and that the data presented is an accurate reproduction. In the absence of this certificate, any electronic evidence cannot be considered, irrespective of its relevance to the case.
- The Supreme Court's ruling in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal[15] (2020) addressed issues arising from the Anvar P.V. decision regarding the presentation of electronic evidence held by third parties, such as social media platforms and telecom companies. The court specifically clarified the provisions concerning the mandatory nature of the 65B certificate, stating that this certificate is required when the original device or system from which evidence is derived is not produced in court. Furthermore, the court established that litigants lacking access to the original device—such as data stored on Google servers—can request judicial intervention to compel the third party to provide the necessary 65B certificate. This ruling effectively balances the critical need for maintaining the authenticity of electronic evidence while acknowledging the practical challenges litigants face in accessing data controlled by third parties.

(2) Responsibility of Intermediaries and the "Safe Harbour"

ital-arrest-beware-of-the-new-cyber-scam-that-alleges-you-of-serious-crime-to-extort-money/articleshow/114762835.cms?from=mdr

[13] *ED arrests 4 in Chinese loan app "fraud" case | TaxTMI.* (2025). TaxTMI. https://www.taxtmi.com/news?id=32235

[14] AIR 2005 SC 3820

[15] AIR 2020 SC 4908

Section 79 of the Information Technology (IT) Act grants "Safe Harbour" protection to intermediaries, shielding them from legal liability for content posted by third parties. This provision is crucial for maintaining the operational integrity of online platforms, allowing them to function without fear of repercussions stemming from user-generated content.

- In the case of Shreya Singhal v. Union of India[16] (2015), the Court interpreted Section 79(3)(b) of the Information Technology Act to clarify the responsibilities of intermediaries concerning online content. It determined that intermediaries are obligated to remove content only when they acquire "actual knowledge" of its illegality through a formal court order or government notification. This ruling affirms that intermediaries are not responsible for independently assessing the legality of the content they host. By doing so, the Court's decision is seen as a significant triumph for free speech, as it mitigates the risk of excessive censorship by platforms motivated by fear of potential legal repercussions.
- X Corp v. Union of India (2024)[17]: In a notable shift towards increased state control over online platforms, the Karnataka High Court upheld the government's authority to issue blocking orders under Section 69A, dismissing X Corp's (formerly Twitter) challenge against such actions. The Court concluded that the government holds the power to block entire accounts, in addition to specific tweets, particularly when matters of national security are at stake. Furthermore, the ruling reinforced the secrecy surrounding the review committee responsible for these decisions, indicating a significant judicial deference to the executive branch regarding the maintenance of public order in online spaces.

(3) Personality Rights and Deepfake Technology

Courts have begun to address the issue of deepfakes by expanding the common law notion of "Personality Rights," as there is currently no specific legislation prohibiting such technology.

- Anil Kapoor v. Union of India[18] (2023): The Delhi High Court granted a broad injunction safeguarding the actor's name, image, voice, and "persona" against unauthorized replication through artificial intelligence (AI). The Court acknowledged the risks posed by AI-generated deepfakes, highlighting that they result in "diminution of personality," which is a harm separate from defamation. This ruling prohibits the use of AI technology to produce commercial merchandise or misleading videos utilizing the actor's likeness.
- Sadhguru Jaggi Vasudev Case[19] (2025) involves the issue of deepfake videos that were utilized to promote fraudulent investment schemes. In response to this issue, the Delhi High Court issued a directive to Google requiring it to remove not just the specific URLs referenced in the case but also to engage in proactive measures to leverage technology aimed at identifying and eliminating similar misleading content. This shift represents a significant transformation from the traditional "notice-and-takedown" approach to a more proactive enforcement model that obligates platforms to monitor and police content actively.

(4) Essential Systems and Cyber Terrorism

The AIIMS Ransomware Attack in 2022 marked a significant point in the threat landscape, illustrating the intersection of individual fraud and national security. Hackers encrypted the data of the All-India Institute of Medical Sciences (AIIMS), demanding a large ransom. In response, the Delhi Police applied Section 66F of the IT Act concerning Cyber Terrorism, as the attack targeted a key national health institute, thus threatening the unity and security of India. This incident revealed the vulnerabilities in India's Critical Information Infrastructure (CII), despite the existence of the National Critical Information Infrastructure Protection Centre (NCIIPC). The operational weaknesses of various government entities were spotlighted, as similar cyber-attacks on organizations

[16] AIR 2015 SC 1523
[17] Writ Petition No. 7405 of 2025
[18] CS(COMM) 652/2023
[19] CS(COMM) 578/2025

like Oil India[20] and SpiceJet[21] have shown that such attacks can lead to significant real-world physical consequences.

VII. CONCLUSION

The study of India's cybercrime scene reveals a dynamic and quickly changing ecosystem shaped by legislative changes. The adoption of the Bharatiya Nyaya Sanhita affords law enforcement greater definitions of organized crime, perhaps assisting the dismantling of criminal syndicates like those in Mewat. The court has reacted to this scenario by adopting the "Arjun Panditrao" and "Anil Kapoor" doctrines, trying to solve difficulties relating to evidence and rights in the context of digital crimes. A low 9% recovery rate in technologically savvy Karnataka demonstrates the stark discrepancy between legal frameworks and the reality of enforcement notwithstanding these developments. This statistic demonstrates how the velocity of cybercrime outstrips the law's procedural pace, making legal solutions inadequate. Additionally, frauds like "Digital Arrest" use not technical competence but rather the psychological weaknesses of victims who are frequently uninformed of their rights and the court procedure, further complicating issues in the battle against cybercrime.

REFERENCE

[1] Kumar, S., & Kaur, G. (2024). Cyber Crimes & Laws (3rd ed.). Whitesmann Publishing.
[2] Deshpande, B. A. (2019). Text Book on Cyber Law (1st ed.). Central Law Publications.
[3] Fatima, T. (2011). Cyber Crimes (1st ed.). Eastern Book Company.
[4] Mohsin, K. (2020). Global Perspective of Cyber Crimes and Related Laws. SSRN Electronic Journal, 23. https://doi.org/10.2139/ssrn.3673938
[5] Farooqui, M. O., Sarhan, A., & Mustafa, F. (2025). Aviation Cyber Security in India: Legal Gaps, International Frameworks, and Policy Reforms. Yustisia Jurnal Hukum, 14(2), 186. https://doi.org/10.20961/yustisia.v14i2.101653
[6] India. (2022, April 22). Russian Malware Used for Oil India Cyber Attack: Report. Www.ndtv.com; NDTV. https://www.ndtv.com/india-news/russian-malware-used-for-oil-india-cyber-attack-in-assam-report-2911203
[7] ET Online. (2024, October 30). Digital arrest: Beware of the new cyber scam that alleges you of serious crime to extort money. The Economic Times; Economic Times. https://economictimes.indiatimes.com/news/india/digital-arrest-beware-of-the-new-cyber-scam-that-alleges-you-of-serious-crime-to-extort-money/articleshow/114762835.cms?from=mdr

[20] India. (2022, April 22). *Russian Malware Used for Oil India Cyber Attack: Report*. Www.ndtv.com; NDTV. https://www.ndtv.com/india-news/russian-malware-used-for-oil-india-cyber-attack-in-assam-report-2911203

[21] Farooqui, M. O., Sarhan, A., & Mustafa, F. (2025). Aviation Cyber Security in India: Legal Gaps, International Frameworks, and Policy Reforms. *Yustisia Jurnal Hukum*, *14*(2), 186. https://doi.org/10.20961/yustisia.v14i2.101653