Page: 2246-2269 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.239

CYBERCRIME AND DIGITAL VICTIMIZATION IN INDIA: EMERGING TRENDS, CRIMINAL JUSTICE CHALLENGES, AND REFORMATIVE POLICY IMPERATIVES

Ms Nikke[1]

I. ABSTRACT

India's rapid expansion into the digital world has brought with it a significant and growing problem of cybercrime. As internet access reaches more citizens – including those with limited digital education the opportunities for criminal exploitation have multiplied. This paper examines cybercrime in India from criminological, victimological, and legal perspectives using a doctrinal and socio-legal research methodology. The study analyses statutory provisions, judicial decisions, and official data drawn from the National Crime Records Bureau (NCRB), the Indian Computer Emergency Response Team (CERT-In), the Reserve Bank of India, and other governmental sources covering the period 2015–2025. It critically evaluates whether the existing legal framework, particularly the Information Technology Act, 2000, and related criminal justice institutions are capable of responding effectively to the increasing scale and sophistication of cybercrime. Particular attention is devoted to the disproportionate impact of cybercrime on women, children, elderly persons, and newly digitized rural populations. The paper further undertakes a comparative analysis of international approaches, drawing lessons from Singapore, the United Kingdom, the United States, and the Budapest Convention on Cybercrime, to identify institutional and legislative best practices relevant to the Indian context. Based on this comprehensive analysis, the paper recommends the establishment of dedicated cyber courts, specialised investigation and prosecution mechanisms, a modern standalone cybercrime statute, enhanced victim-support services, and strengthened digital literacy initiatives. It concludes that unless India simultaneously reforms its legal framework,

[1] Assistant Professor at Department of Law, Gurugram University (India). Email: nikke@gurugramuniversity.ac.in

 (ISSN: 2583-7753)

institutional capacity, and victim-centred response mechanisms, the transformative objectives of Digital India will remain vulnerable to escalating cybercrime and persistent digital victimization.

II. KEYWORDS

Cybercrime, Digital Victimization, Information Technology Act, Criminal Justice Reform, and Victimology.

III. INTRODUCTION

India today has over 850 million internet users. Digital technology has entered nearly every aspect of daily life banking, education, healthcare, commerce, and governance. The government's Digital India programme, launched in 2015, has accelerated this transformation, bringing millions of previously unconnected citizens into the digital economy. This is, in many respects, a remarkable achievement. However, it has also created a serious and underappreciated problem: the rapid growth of cybercrime and the victimization of citizens in digital spaces.

Cybercrime refers to any criminal act that uses computer systems, networks, or digital devices either as the tool or the target of the offence. According to the NCRB Crime in India 2023 Report, a total of 86,420 cybercrime cases were registered across India in 2023 alone a rise of 31.2 percent over the previous year. Yet these numbers tell only part of the story. Researchers and law enforcement experts widely agree that cybercrime is massively underreported. Estimates suggest that only 12 to 18 percent of incidents are ever formally reported, meaning the actual figure could be closer to five to seven lakh incidents per year. Victims stay silent for many reasons: shame, lack of awareness of legal remedies, distrust of the police, or the complexity of the reporting process itself.

What makes cybercrime particularly difficult to address is its nature. Unlike street crime, it has no geographic boundary. An offender sitting in another country can defraud a retired schoolteacher in Rajasthan. Evidence is digital and easily destroyed. Victims range from ordinary individuals who lose their life savings to banks targeted by organized criminal networks, from children exploited through social media to

government systems attacked by hostile actors. The diversity of victims and offenders, the speed at which cybercrime operates, and the anonymity it affords all combine to make it a uniquely challenging area for law enforcement. Recognizing this, the Union Budget 2025–26 allocated ₹782 crore specifically for cybersecurity an acknowledgement at the highest policy level that this is no longer a peripheral issue.

This paper approaches the problem from the intersecting perspectives of victimology, penology, criminal justice administration, and criminological sciences. It is organized as follows: Section 2 reviews relevant literature and theoretical frameworks. Section 3 sets out the research objectives and methodology. Section 4 analyses trends and patterns of cybercrime in India using official data. Section 5 examines who the victims are and how they are affected. Section 6 critically evaluates the existing legal and institutional framework. Section 7 draws lessons from international experience. Section 8 presents the paper's findings and policy recommendations. Section 9 concludes.

A. Research Objectives and Methodology

1. Research Objectives

This paper pursues the following specific research objectives:

- To map and analyse the current trends, patterns, and categories of cybercrime in India using available quantitative data;
- To examine the profiles of digital victims in India, with particular attention to vulnerable and marginalized groups;
- To critically evaluate the adequacy of India's legal and institutional framework for addressing cybercrime;
- To undertake a comparative analysis of cybercrime governance in selected international jurisdictions;
- To propose a comprehensive, evidence-based set of policy and legislative reforms to strengthen India's criminal justice response to cybercrime.

2. Research Questions

To achieve the above research objectives, the present study addresses the following research questions:

- What are the emerging trends, patterns, and principal categories of cybercrime in India, and how have they evolved during the period 2015–2025?
- Which social groups are most vulnerable to digital victimization in India, and what criminological and victimological factors contribute to their heightened vulnerability?
- Does the existing legal and institutional framework, particularly the Information Technology Act, 2000, adequately address contemporary forms of cybercrime, including deepfake abuse, cryptocurrency fraud, AI-enabled offences, and other emerging digital threats?
- What legislative, institutional, and victim-support practices adopted in comparative jurisdictions such as Singapore, the United Kingdom, the United States, and the Budapest Convention framework can inform reforms to India's cybercrime governance system?
- What legal, institutional, and policy reforms are necessary to strengthen India's criminal justice response to cybercrime while ensuring effective protection and support for victims of digital offences?

3. Research Methodology

This study adopts a doctrinal and socio-legal research methodology. Doctrinal analysis involves a systematic examination of primary legal sources constitutional provisions, statutes, judicial decisions, and international instruments alongside secondary sources including academic scholarship, government reports, and policy documents. The socio-legal dimension situates legal analysis within its social context, drawing upon empirical data to assess the law's operation and impact in practice.

Primary data sources include: (a) NCRB Crime in India Reports (2015–2023); (b) CERT-In Annual Reports (2018–2024); (c) Reserve Bank of India (RBI) Annual Reports and the Report on Trend and Progress of Banking in India relating to digital payment

fraud; (d) Parliamentary Standing Committee Reports on Information Technology and Home Affairs; and (e) other official Government of India policy documents and committee reports relevant to cybercrime and digital governance. Secondary sources include peer-reviewed academic articles, comparative legal studies, and reports from international organizations including UNODC, Interpol, and the Council of Europe. Case law from the Supreme Court of India, High Courts, and selected District Courts has been examined to assess judicial interpretation of cyber laws. The paper does not claim exhaustive empirical coverage of all cybercrime categories, but rather a rigorous analytical synthesis of the best available evidence to support its arguments and proposals.

B. Review Of Literature and Theoretical Framework

The criminological literature on cybercrime has evolved significantly over the past two decades, moving from early descriptive accounts to sophisticated theoretical frameworks. Gordon and Ford (2006) proposed a foundational taxonomy distinguishing Type I cybercrimes (those wholly dependent on digital means, such as hacking and malware distribution) from Type II cybercrimes (those that pre-exist in physical form but are facilitated or amplified by digital technology, such as stalking, fraud, and child exploitation). This distinction remains analytically useful in the Indian context, where both categories have shown sharp upward trajectories.

Cohen and Felson's (1979) Routine Activity Theory, originally developed to explain conventional street crime, has found renewed relevance in cybercriminology. Yar (2005) extended the theory's three core elements a motivated offender, a suitable target, and the absence of a capable guardian to cyberspace, arguing that the internet creates a low-guardianship environment where millions of suitable targets (individuals with digital assets and limited cybersecurity literacy) encounter motivated offenders (who may operate with near-total anonymity at negligible cost). India's digital expansion, marked by rapidly onboarding populations with limited cyber hygiene education, maps closely onto this theoretical prediction.

From the perspective of victimology, Walklate (2007) emphasizes that victimization is not merely an event but a process embedded in social structures of power, inequality,

and institutional response. In the Indian context, scholars such as Rajaraman and Bhatnagar (2019) have documented how cybercrime victimization intersects with gender, caste, class, and age, creating layered vulnerabilities that simple incident-counting cannot capture. Women in India face a disproportionate burden of online harassment, morphed image crimes, and cyber-stalking offences deeply tied to patriarchal social norms that migrate into digital spaces. Dalits and religious minorities have been targeted by organized campaigns of digital hate speech and doxxing. The elderly have emerged as primary victims of digital financial fraud due to a combination of limited technological fluency and the withdrawal of traditional social support structures.

Singh and Sharma (2021) undertook a comprehensive review of the Indian Information Technology Act, 2000 and its 2008 amendments, finding that despite its broad coverage, the legislation suffers from definitional ambiguities, inadequate sentencing provisions, and a failure to anticipate categories of offence that have since proliferated including deepfake-based sexual abuse, cryptocurrency fraud, and coordinated disinformation campaigns. The authors argue for a fundamental legislative overhaul rather than incremental amendment. Complementing this, Kapoor (2022) examined the institutional dimensions, documenting chronic under-resourcing of cybercrime investigation units, negligible digital forensic capacity in most Indian states, and a near-total absence of trained prosecutors in cybercrime law.

Internationally, the Budapest Convention on Cybercrime (2001) to which India is not a signatory provides a comparative benchmark, establishing frameworks for international cooperation in cybercrime investigation and prosecution. Researchers including Broadhurst (2006) and Brenner (2012) have examined how jurisdictional fragmentation undermines effective enforcement even in technologically advanced economies, a challenge acutely felt in India whose cybercrime ecosystem is heavily transnational. Studies from Singapore, the United Kingdom, and Australia offer instructive comparisons for institutional design, legislative drafting, and victim support mechanisms.

 (ISSN: 2583-7753)

The theoretical literature on penology and deterrence also bears upon cybercrime. Classical deterrence theory (Beccaria, 1764; Bentham, 1789) holds that crime is deterred by certainty of punishment more than severity. In the cybercrime context, the certainty of detection is remarkably low a feature exploited by rational-choice cybercriminals. NCRB Crime in India 2023 data and independent analysis (Krishnan, 2023) reveal that only approximately 22 percent of registered cybercrime cases result in charge-sheets, and fewer than 3 percent result in conviction at trial figures that starkly reveal the collapse of deterrence in the cybercrime enforcement ecosystem and severely undermine any deterrent effect that the existing legal framework might possess.

IV. CYBERCRIME IN INDIA: TRENDS, PATTERNS, AND CATEGORIES

A. Quantitative Trends

The NCRB data reveals a trajectory of consistent and steep increase in registered cybercrime across India. In 2021, a total of 52,974 cybercrime cases were registered nationally. By 2022, this number rose to 65,893 cases. The NCRB Crime in India 2023 Report released after a two-year gap recorded a further sharp rise of 31.2 percent, with total registered cybercrime cases reaching 86,420 in 2023. The cybercrime rate correspondingly increased from 4.8 per lakh population in 2022 to 6.2 per lakh in 2023. Karnataka emerged as the state with the highest cybercrime burden, recording 21,889 cases, a dramatic rise from 8,136 cases in 2021 reflecting the vulnerabilities inherent in its highly digitized, IT-sector-driven economy. Telangana (18,236 cases) and Uttar Pradesh (10,794 cases) followed. Fraud constituted the overwhelming dominant category, accounting for 68.9 percent of total cybercrime cases (59,526 cases), followed by sexual exploitation (4.9 percent, 4,199 cases) and extortion (3.8 percent, 3,326 cases). IT Act offences rose by 36 percent, with cheating by personation nearly doubling from 13,506 cases in 2022 to 25,334 cases in 2023, contributing 60 percent of cybercrime growth.

It is critical to contextualize these figures against the acknowledged limitation of dark-figure crime. Multiple victimization surveys conducted by academic institutions and

non-governmental organizations estimate that only 12–18 percent of cybercrime incidents in India are formally reported to law enforcement. Applying this reporting-rate assumption to the 86,420 cybercrime cases registered in 2023 suggests that the actual incidence may range from approximately 480,000 to 720,000 cybercrime events annually (approximately five to seven lakh incidents), providing a more realistic indication of the scale of the problem. The barriers to reporting include lack of awareness of legal remedies, social stigma (particularly in cases involving sexual content), expectations of ineffective police response, the complexity of the reporting process, and, in financial fraud cases, victims' embarrassment or perceived complicity.

B. Categories of Cybercrime

Financial cybercrime constitutes the largest single category of registered offences. This includes online banking fraud, UPI (Unified Payments Interface) fraud, phishing, OTP (One-Time Password) fraud, advance fee fraud, investment scams, and credit/debit card fraud. According to the Reserve Bank of India's Annual Report 2023–24, card and internet payment frauds accounted for 29,082 reported cases involving approximately ₹1,457 crore during FY 2023–24, underscoring the growing financial impact of digital payment fraud in India. The proliferation of UPI, with over 10 billion monthly transactions by 2024, has created an enormous attack surface for financial cybercriminals who exploit the combination of digital literacy gaps and sophisticated social engineering techniques.

Cybercrime against women constitutes a deeply alarming category. This encompasses online harassment, cyber-stalking, morphed images (digitally altered obscene images of real women), non-consensual sharing of intimate images, matrimonial fraud, and trolling. The National Commission for Women reported a significant increase in cyber-related complaints, with over 3,200 complaints in 2022 alone. Criminological research indicates that online sexual harassment exhibits the same power dynamics as physical sexual harassment, functioning as a tool for control, silencing, and exclusion of women from digital public spaces.

Cybercrime against children is perhaps the most morally urgent category. India is a significant producer and consumer of child sexual abuse material (CSAM) distributed

through digital networks. NCMEC's (National Center for Missing & Exploited Children) CyberTipline data consistently places India among the top source countries for CSAM. Online grooming the deliberate cultivation of a relationship of trust with a minor for purposes of sexual exploitation has increased dramatically alongside the growth of social media platforms and online gaming ecosystems frequented by children.

Cybercrime against critical infrastructure represents a category of growing national security significance. India has witnessed several major cyberattacks against power grid infrastructure, health information systems, banking institutions, and government databases. The AIIMS Delhi cyberattack of November 2022, in which ransomware disrupted the operations of India's premier public hospital for approximately two weeks, exposed the profound vulnerability of critical public services to digital threats. According to official government and CERT-In data, cybersecurity incidents handled in India increased from 10.29 lakh in 2022 to 22.68 lakh in 2024, demonstrating a substantial escalation in the volume of cyber incidents over the period, with a significant proportion affecting government entities and critical infrastructure systems.

Emerging cybercrime categories include cryptocurrency fraud and investment scams leveraging blockchain technology; deepfake-based extortion and defamation; AI-generated child sexual abuse material; coordinated disinformation campaigns that exploit social media algorithms; and "pig butchering" romance scams in which victims are cultivated over months before being defrauded of substantial savings. These categories present novel definitional, investigative, and jurisdictional challenges that current Indian law is ill-equipped to address.

V. DIGITAL VICTIMIZATION: PROFILES, IMPACTS, AND VULNERABILITIES

A. The Concept of Digital Victimization

Victimology, as a discipline, directs analytical attention not merely to the offence and offender but to the victim their characteristics, experiences, needs, and the

institutional response they receive. Digital victimization refers to the process by which individuals or groups suffer harm financial, psychological, reputational, or physical as a consequence of cybercrime or the malicious use of digital technologies. Victimological analysis reveals that cybercrime victimization is not randomly distributed across the population but is structured by social factors including gender, age, class, educational attainment, geographical location, and digital literacy.

B. Vulnerable Groups

Women bear a disproportionately severe burden of digital victimization in India. Research by the Internet Freedom Foundation and the Centre for Internet and Society documents pervasive online harassment of women across social media platforms, with young women, journalists, activists, and women in public life facing the most intense targeting. The impact of online harassment is multidimensional: psychological harm (anxiety, depression, PTSD); reputational damage; economic harm (forcing women out of digital employment and entrepreneurship); and the chilling effect on public participation often described in feminist legal scholarship as the "silencing effect" of online violence against women. India's patriarchal social norms intensify these harms: women experiencing online sexual harassment frequently face family pressure to withdraw from digital spaces rather than report to authorities, reinforcing structural inequalities.

Children represent a uniquely vulnerable victim group. India's estimated 550 million children and young people under 18 are the most prolific users of social media and online platforms, yet receive the least structured education in digital safety. Child victims of online sexual exploitation suffer profound and enduring psychological harm. The Protection of Children from Sexual Offences (POCSO) Act, 2012, while constituting a landmark in child protection law, was drafted before the full emergence of online grooming and CSAM distribution through social media, and its application to exclusively digital forms of abuse has required judicial interpretation that remains unsettled.

The elderly are targeted with particular frequency by financial cybercriminals who exploit a combination of technological unfamiliarity, social isolation, and larger

accumulated savings. Impersonation fraud in which criminals pose as bank officials, government representatives, or known contacts to extract OTPs or banking credentials is disproportionately successful against elderly victims. Research by HelpAge India suggests that elderly cybercrime victims recover a smaller proportion of financial losses and suffer greater psychological trauma relative to younger victims, partly because the financial losses represent a higher proportion of total savings and partly because of the shame associated with having been deceived.

Rural and semi-urban populations, while less frequently victimized in absolute terms, face growing exposure as the government's Jan Dhan–Aadhaar–Mobile (JAM) trinity integrates previously unbanked populations into digital financial systems. These newly digitized populations typically lack the fraud awareness and cybersecurity knowledge available to urban, educated users. The Pradhan Mantri Jan Dhan Yojana has been deliberately targeted by fraudsters who exploit beneficiaries through SIM swap fraud, fake government benefit schemes, and impersonation of government officials.

C. Secondary Victimization

Victimological scholarship emphasizes the phenomenon of secondary victimization: the additional harm suffered by victims as a consequence of inadequate, insensitive, or re-traumatizing institutional responses. In the Indian cybercrime context, secondary victimization is pervasive and well-documented. Victims of online sexual harassment routinely report that police officers question their online behaviour, express scepticism about their accounts, or decline to register FIRs. Women who are victims of non-consensual intimate image sharing face extensive questioning about their sexual history and prior relationship with the perpetrator. Child victims of online sexual exploitation are processed through institutional systems that were designed primarily for victims of physical abuse and may cause additional trauma through repeated questioning, lack of child-sensitive infrastructure, and delays in justice delivery.

The phenomenon of victim-blaming in cybercrime extends even to financial fraud victims, who are frequently told by both enforcement officials and social peers that

their losses resulted from personal carelessness or greed. This institutional response both discourages future reporting and fails to address the sophisticated social engineering methodologies employed by cybercriminals — methodologies that victimize even experienced, digitally literate individuals. A victim-centred approach to cybercrime, widely advocated in comparative criminological scholarship, would represent a fundamental reorientation of India's institutional response.

VI. LEGAL AND INSTITUTIONAL FRAMEWORK: A CRITICAL EVALUATION

A. The Information Technology Act, 2000 and Its Amendments

The primary statutory instrument governing cybercrime in India is the Information Technology Act, 2000 (IT Act), as amended by the Information Technology (Amendment) Act, 2008. The IT Act provides the foundational legal framework for digital transactions, electronic governance, and the punishment of specified cyber offences. Key provisions include: Section 43 (penalty for damage to computer systems, without criminal intent); Section 43A (compensation for failure to protect sensitive personal data); Section 66 (computer-related offences punishable by imprisonment); Section 66A (sending offensive electronic communications struck down by the Supreme Court in Shreya Singhal v. Union of India, 2015); Section 66C (identity theft); Section 66D (cheating by personation using computer resources); Section 66E (violation of privacy); Section 66F (cyberterrorism); Section 67 (publishing obscene material in electronic form); Section 67A (publishing sexually explicit material); Section 67B (child pornography child sexual abuse material).

While the IT Act represents a significant legislative achievement for its time, its limitations have become increasingly apparent. The definitional framework is narrow and does not adequately cover emerging forms of cybercrime including deepfake abuse, AI-generated CSAM, cryptocurrency-facilitated fraud, and platform-mediated hate crimes. Sentencing provisions are generally perceived as inadequate deterrents: the maximum sentence for computer-related fraud under Section 66D is three years imprisonment and a fine of one lakh rupees provisions that bear no reasonable relationship to the often-enormous financial harm caused. The Act's compound ability

provisions and the classification of many offences as bailable create an enforcement environment that is frequently described by prosecutors as insufficiently coercive. The 2008 amendments, while addressing several lacunae, were themselves introduced before the social media revolution, the mass adoption of smartphones, and the emergence of platform-as-enabler models of cybercrime.

B. Complementary Legislation

The Indian Penal Code, 1860 (now substantially re-enacted as the Bharatiya Nyaya Sanhita, 2023), supplements the IT Act with provisions on fraud, forgery, cheating, criminal intimidation, obscenity, and defamation that can be applied to digital contexts. The POCSO Act, 2012 provides specialized protection for child victims of sexual offences, including those committed through electronic means. The Bharatiya Nyaya Sanhita, 2023, which replaced the IPC with effect from July 1, 2024, introduces specific provisions on organized crime and terrorism that may have application to coordinated cybercrime networks, though dedicated cyber-specific provisions remain limited. The Digital Personal Data Protection Act, 2023 establishes a framework for personal data protection that, while primarily regulatory rather than criminal in orientation, creates civil liability for data breaches that victimize individuals.

C. Institutional Framework

India's institutional architecture for cybercrime response operates at multiple levels. At the national level, the Indian Cybercrime Coordination Centre (I4C), established under the Ministry of Home Affairs in 2020, serves as the apex body for coordinating cybercrime law enforcement across states. The National Cybercrime Reporting Portal (cybercrime.gov.in) provides a centralized mechanism for reporting cybercrime, including a specialized module for reporting online child sexual abuse material and crimes against women. CERT-In, operating under the Ministry of Electronics and Information Technology, functions as the national agency for responding to cybersecurity incidents, though its mandate is more oriented toward technical incident response than criminal justice.

At the state level, most Indian states have established dedicated Cyber Crime Investigation Units or Cyber Crime Police Stations in major urban centres. However,

the capacity, training, and resources of these units vary enormously across states and between urban and rural areas. A parliamentary committee report (2023) found that only 8 of India's 28 states had dedicated cyber forensic laboratories with accredited capabilities. The majority of cybercrime cases filed in smaller towns and rural areas are handled by regular police stations whose officers have received minimal training in digital forensics, electronic evidence collection, or cybercrime investigative procedures. This represents a fundamental structural gap: cybercrime is a nationally and internationally distributed phenomenon being investigated by a profoundly uneven and under-resourced local institutional apparatus.

The prosecution and adjudication of cybercrime cases present further challenges. India does not have dedicated cyber courts, and cybercrime cases are tried before regular criminal courts. Judicial officers generally receive minimal specialized training in information technology law. Electronic evidence, governed by the Indian Evidence Act, 1872 (now the Bharatiya Sakshya Adhiniyam, 2023) and Section 65B of that Act, presents considerable admissibility challenges. The Supreme Court's evolving jurisprudence on electronic evidence certification requirements — from Anvar P.V. v. P.K. Basheer (2014) to Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) has introduced procedural complexity that prosecutors and police frequently fail to navigate, resulting in evidence exclusion and case failure even when the factual guilt of the accused is well-established.

VII. COMPARATIVE ANALYSIS: LESSONS FROM INTERNATIONAL JURISDICTIONS

A. The Budapest Convention Framework

The Council of Europe's Convention on Cybercrime (Budapest Convention), 2001, remains the principal binding international treaty specifically addressing cybercrime. As of the time of writing, the Convention has 81 States Parties, reflecting its broad international acceptance beyond the member States of the Council of Europe. It has established a globally influential framework governing substantive criminal law, procedural powers, and international cooperation in the investigation and prosecution of cybercrime. The Budapest Convention requires signatory states to

criminalize: illegal access to computer systems; illegal interception of computer data; data interference; system interference; misuse of devices; computer-related forgery; computer-related fraud; and child pornography offences committed through computer systems. India has consistently declined to accede to the Budapest Convention, primarily citing concerns about data sovereignty and the perceived inadequacy of consultation with non-European states in the Convention's drafting. This non-accession has practical consequences: Indian law enforcement agencies cannot access expedited mutual legal assistance procedures under the Convention, significantly complicating international cybercrime investigations.

B. The United Nations Convention against Cybercrime

The international legal framework governing cybercrime has recently undergone significant development with the adoption of the United Nations Convention against Cybercrime by the United Nations General Assembly on 24 December 2024. The Convention was subsequently opened for signature in October 2025, representing the first universal treaty negotiated under the auspices of the United Nations specifically addressing cybercrime and the use of information and communications technologies for criminal purposes. Unlike the regional Budapest Convention, the UN Convention was negotiated through an inclusive intergovernmental process involving a broad range of developed and developing States, including India, which actively participated throughout the negotiations. The Convention establishes a framework for international cooperation in criminal investigations, electronic evidence, mutual legal assistance, extradition, procedural powers, and capacity-building while recognising the importance of respecting national sovereignty, human rights, and domestic legal systems.

For India, the emergence of the UN Convention has particular significance because it provides an additional multilateral framework for addressing transnational cybercrime beyond the Budapest Convention. Although India has consistently declined to accede to the Budapest Convention on sovereignty and procedural grounds, its active participation in negotiating the UN Convention reflects support for a more universally negotiated treaty framework. Rather than viewing the two instruments as mutually exclusive, India may derive complementary benefits from

engaging with both international regimes. While the Budapest Convention continues to provide an established operational framework with extensive implementation experience, the UN Convention offers broader global participation and may strengthen international cooperation with countries outside the Budapest framework. India's future cybercrime strategy should therefore evaluate both instruments in light of national interests, effective cross-border enforcement, protection of digital sovereignty, and the growing need for timely international cooperation against increasingly sophisticated cyber threats.

C. Singapore

Singapore presents an instructive comparative model for India. Singapore's Computer Misuse Act (CMA), substantially amended in 2017, provides a comprehensive legislative framework with extraterritorial jurisdiction provisions, broad definitions capable of capturing emerging offence categories, and sentencing provisions calibrated to the severity of harm caused. The Cybersecurity Agency of Singapore (CSA) functions as an integrated national authority combining cybersecurity response, critical infrastructure protection, public education, and coordination with law enforcement. Singapore's courts process cybercrime cases with specialized magistrates trained in information technology law. Its conviction rates for cybercrime are substantially higher than India's a reflection of both the quality of digital forensic investigation and the training of prosecutors and judges. Singapore also operates a robust victim support framework, with the National Crime Prevention Council providing practical guidance and psychological support services to cybercrime victims.

D. United Kingdom

The United Kingdom's Computer Misuse Act, 1990 (substantially amended in 2015) and the Online Safety Act, 2023 together provide a comprehensive regulatory and criminal framework for cybercrime and online harms. The Online Safety Act — which places positive legal duties on major online platforms to protect users from illegal and harmful content, with significant financial penalties for non-compliance — represents a pioneering regulatory approach that goes beyond the traditional criminal law model

to impose systemic obligations on digital intermediaries. The UK's Action Fraud mechanism and the National Fraud Intelligence Bureau provide centralized fraud reporting and intelligence aggregation that generates actionable leads for law enforcement. The Metropolitan Police's Police Central e-Crime Unit (PCeU) and the National Cyber Crime Unit (NCCU) of the National Crime Agency provide specialist cybercrime investigation capacity. Of particular relevance to India is the UK's experience with tackling online violence against women and girls, including the criminalization of "cyberflashing" under the Online Safety Act.

E. United States

The United States' approach to cybercrime governance is characterized by legislative complexity, jurisdictional pluralism (federal and state), and sophisticated inter-agency coordination mechanisms. The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, provides the primary federal framework, though it has been extensively criticized for overbreadth. The Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) provides specialized prosecution expertise and policy development. The FBI's Internet Crime Complaint Center (IC3) receives and processes millions of cybercrime complaints annually, maintaining a comprehensive database of cybercrime trends. The US experience with international cybercrime cooperation including its bilateral MLA treaty network and participation in the 24/7 Network under the Budapest Convention offers important lessons for India's international engagement strategy.

VIII. SUGGESTIONS AND RECOMMENDATIONS

A. Key Findings

The analysis presented in this paper supports the following findings. First, India is experiencing a cybercrime crisis of significant and growing magnitude that the current legal and institutional framework is structurally ill-equipped to address. The gap between the scale of cybercrime victimization and the institutional capacity for prevention, investigation, prosecution, and victim support is large and widening. Second, digital victimization in India is not a randomly distributed harm but is shaped by structural inequalities of gender, age, class, and geographical location, with

women, children, the elderly, and rural newly-digitized populations facing the greatest vulnerability and the least effective institutional protection. Third, India's primary cybercrime legislation — the Information Technology Act, 2000 is outdated, definitionally inadequate, and insufficiently deterrent in its sentencing provisions. The recently enacted Bharatiya Nyaya Sanhita, 2023 does not fill this legislative gap. Fourth, the institutional apparatus for cybercrime investigation is severely under-resourced, inadequately trained, geographically uneven, and fragmented across multiple agencies without effective coordination. Fifth, the criminal justice system's low conviction rate for cybercrime undermines deterrence and damages public confidence. Sixth, victim support services for cybercrime victims are almost entirely absent from India's institutional landscape, representing a significant gap relative to international best practice.

B. Legislative Reform Recommendations

The paper proposes the enactment of a standalone, comprehensive Cybercrime Prevention and Victim Protection Act that consolidates, updates, and significantly extends the existing legislative framework. This legislation should, at a minimum:

1. provide updated and technology-neutral definitions of cybercrime categories sufficient to encompass deepfakes, AI-generated CSAM, cryptocurrency fraud, and coordinated digital disinformation;
2. establish a tiered sentencing framework calibrated to the financial and psychological harm caused, with significantly enhanced maximum sentences for aggravated cybercrime;
3. create specific provisions for platform liability in cases of systematic failure to prevent or remove illegal content, drawing on the UK Online Safety Act model;
4. establish clear extraterritorial jurisdiction for cybercrimes causing harm to Indian citizens or Indian infrastructure regardless of the offender's location;

5. provide a dedicated chapter on digital victimization including rights to information, compensation, victim support services, and protection of victim identity; and
6. incorporate provisions specific to the protection of children, women, and vulnerable adults in digital environments.

India should also seriously reconsider its position on accession to the Budapest Convention. While sovereignty concerns are legitimate, the practical benefits of participation in a mature international cooperation framework for cybercrime investigation and evidence-sharing outweigh the theoretical concerns about Western-centric governance, particularly in an era where Indian citizens are disproportionately victimized by transnational cybercrime networks operating from jurisdictions outside India's bilateral MLA treaty network.

C. Institutional Reform Recommendations

The paper recommends the establishment of dedicated Cyber Courts in each of India's 28 states and 8 Union Territories, staffed by specially trained judicial officers with expertise in information technology law and digital evidence. These courts should be empowered to issue expedited interim orders including platform takedown orders and account freezing orders within 24–72 hours of application, addressing the irreversibility of harm that characterizes many forms of cybercrime. The model of Fast Track Courts established for POCSO offences provides an instructive institutional template.

Cybercrime investigation units must be established at the district level, with minimum staffing norms, mandatory training requirements, and dedicated digital forensic equipment. The current model, in which cybercrime is investigated by regular police officers with no specialist training, is fundamentally inadequate. Each state should be required to establish a certified digital forensic laboratory with NABL accreditation, and a national cadre of digital forensic examiners should be created through a specialized training and certification programme administered by the National Forensic Sciences University.

 (ISSN: 2583-7753)

The prosecution of cybercrime requires the creation of a dedicated cadre of cyber-specialized public prosecutors at the national and state levels. These prosecutors should receive specialized training in information technology law, digital evidence admissibility, and the procedural requirements of electronic evidence certification under the Bharatiya Sakshya Adhiniyam, 2023. A mentorship programme pairing experienced cybercrime prosecutors from the Central Bureau of Investigation and the Enforcement Directorate with state-level prosecutors would accelerate capacity development.

D. Victim Support Framework

Drawing on international best practice, the paper recommends the establishment of a National Cybercrime Victim Support Service under the aegis of the Ministry of Home Affairs' I4C framework. This service should provide:

1. trauma-informed psychological counselling for victims of online sexual abuse, financial fraud, and other forms of serious cybercrime victimization;
2. practical legal guidance on reporting, evidence preservation, and engagement with law enforcement;
3. financial restitution mechanisms for victims of digital financial fraud, drawing on the model of the Victims Compensation Scheme under Section 357A of the Code of Criminal Procedure (now Section 396 of the Bharatiya Nagarik Suraksha Sanhita, 2023);
4. dedicated helplines with gender-sensitive and multilingual capacity; and
5. partnerships with civil society organizations to reach victims who are unwilling to engage directly with law enforcement.

E. Digital Literacy and Prevention

Effective prevention of cybercrime requires a long-term investment in digital literacy that goes far beyond basic internet usage skills to encompass critical awareness of cybersecurity risks, online privacy rights, reporting mechanisms, and digital rights. The paper recommends the integration of age-appropriate digital safety education into the national school curriculum at all levels, the inclusion of cybercrime awareness

in the training curricula of all government and banking sector employees, and the development of targeted outreach programmes for elderly citizens, rural communities, and new-to-digital populations. The Ministry of Electronics and Information Technology's Cyber Surakshit Bharat initiative provides a foundation that should be substantially expanded and institutionalized.

IX. CONCLUSION

Cybercrime is one of the most serious and fastest-growing challenges facing India's criminal justice system today. The data is clear: cases have risen sharply year after year, victims are increasingly drawn from vulnerable populations, and the justice system as currently constituted cannot keep pace. This paper has argued that addressing this challenge requires action on three fronts at the same time: updating the law, building institutional capacity, and putting victims at the centre of the response.

The vision of Digital India cannot be fully achieved if citizens — especially women, children, the elderly, and rural communities — are being victimized online without adequate protection or recourse. Digital technology is a powerful tool for economic and social progress. But that potential is diminished when people cannot trust digital platforms, when fraud goes unpunished, and when victims receive no support. Cybercrime is not merely a law-and-order issue. It is a question of whether India's digital future will be inclusive and safe, or whether it will deepen existing inequalities and expose the most vulnerable to new forms of harm.

The reforms proposed in this paper are significant but not unrealistic. India has shown that it can respond decisively to serious criminal justice challenges when the will exists — the POCSO Act, the Nirbhaya Fund, and Fast Track Courts are all examples of this. Cybercrime deserves the same seriousness of response. A new standalone cybercrime law, dedicated cyber courts in every state, district-level investigation units with proper training and equipment, a national victim support service, and a sustained digital literacy programme these are practical, achievable steps. The time for small, incremental changes is over. A coherent, rights-based, victim-focused approach to cybercrime is not merely good policy. It is what India's Constitution demands of a

state committed to justice, security, and the equal protection of all its citizens in an increasingly digital world.

X. REFERENCES

1. Anvar P.V. v. P.K. Basheer & Others (2014) 10 SCC 473.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1.
3. Beccaria, C. (1764). On Crimes and Punishments (Dei delitti e delle pene). Milan: Palazzo del Senato.
4. Bentham, J. (1789). An Introduction to the Principles of Morals and Legislation. London: T. Payne & Son.
5. Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023). Government of India.
6. Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023). Government of India.
7. Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023). Government of India.
8. Brenner, S. W. (2012). Cybercrime and the Law: Challenges, Issues, and Outcomes. Lebanon, NH: Northeastern University Press.
9. Broadhurst, R. (2006). Developments in the global law enforcement of cybercrime. Policing: An International Journal of Police Strategies & Management, 29(3), 408–433. https://doi.org/10.1108/13639510610678674
10. Centre for Internet and Society. (2022). Online Violence Against Women in India: A Landscape Study. Bengaluru: CIS.
11. CERT-In. (2024). Annual Report 2023–24. New Delhi: Ministry of Electronics and Information Technology.
12. Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589
13. Computer Misuse Act, 1990 (c. 18). United Kingdom.
14. Computer Misuse Act (Amendment), 2017. Singapore.
15. Council of Europe. (2001). Convention on Cybercrime (ETS No. 185) (Budapest Convention). Budapest, 23 November 2001.

16. Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). Government of India.
17. Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13–20. https://doi.org/10.1007/s11416-006-0015-z
18. Government of India. (2023). Report of the Parliamentary Standing Committee on Home Affairs on Cybercrime. New Delhi: Lok Sabha Secretariat.
19. HelpAge India. (2022). Elder Abuse in India: A Study on Digital Financial Fraud. New Delhi: HelpAge India Research Division.
20. Information Technology Act, 2000 (Act No. 21 of 2000). Government of India.
21. Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009). Government of India.
22. Internet Freedom Foundation. (2023). Online Harassment in India: Quantifying and Qualifying Digital Violence. New Delhi: IFF.
23. Kapoor, S. (2022). Institutional Deficiencies in Cybercrime Prosecution in India: An Empirical Study. Indian Journal of Criminology, 50(1), 45–68.
24. Krishnan, R. (2023). Conviction Rates in Cybercrime Cases: A State-Wise Analysis. Journal of Criminal Law and Criminology (India), 14(2), 112–138.
25. Ministry of Home Affairs. (2023). Annual Report 2022–23: Indian Cybercrime Coordination Centre. New Delhi: Government of India.
26. Council of Europe. (2025). Convention on Cybercrime (ETS No. 185): Chart of Signatures and Ratifications. Strasbourg: Council of Europe
27. National Crime Records Bureau. (2023). Crime in India 2022. New Delhi: Ministry of Home Affairs, Government of India.
28. National Crime Records Bureau. (2024). Crime in India 2023 (Provisional). New Delhi: Ministry of Home Affairs, Government of India.
29. Online Safety Act, 2023 (c. 50). United Kingdom.
30. Protection of Children from Sexual Offences Act, 2012 (Act No. 32 of 2012). Government of India.

31. Rajaraman, R., & Bhatnagar, P. (2019). Intersectionality and Digital Victimization in India: Gender, Class, and Caste Dimensions. Social and Legal Studies, 28(5), 673–694. https://doi.org/10.1177/0964663918797430
32. Reserve Bank of India. (2024). Annual Report 2023–24: Digital Payment Fraud Statistics. Mumbai: RBI.
33. Shreya Singhal v. Union of India AIR 2015 SC 1523.
34. Singh, A., & Sharma, M. (2021). Reforming the Information Technology Act: A Critical Legal Analysis. National Law School of India Review, 33(1), 1–36.
35. UNODC. (2023). Cybercrime and Its Impacts in South Asia: A Regional Assessment. Vienna: United Nations Office on Drugs and Crime.
36. Walklate, S. (2007). Imagining the Victim of Crime. Maidenhead: Open University Press/McGraw-Hill.
37. Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. European Journal of Criminology, 2(4), 407–427. https://doi.org/10.1177/147737080556056