VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

THE DIGITAL TURN IN WHITE-COLLAR CRIMES: CYBER FRAUDS AND HUMAN RIGHTS VULNERABILITIES IN INDIA

- Mr. Ananda Vishnu[1] & Ms. T. Vaishali[2]

Abstract

The proliferation of digital technologies has fundamentally transformed the landscape of white-collar crime in India, creating sophisticated mechanisms for financial fraud that exploit technological infrastructure and human vulnerabilities. This paper examines the intersection of cyber frauds, digital crimes, and human rights violations in contemporary India, analyzing the structural vulnerabilities in both legal frameworks and digital governance mechanisms. Drawing on recent empirical data, case law, and institutional responses, this research argues that India's existing legal framework-centered on the Information Technology Act, 2000-inadequately addresses the nexus between cybercriminal activity and systemic human rights erosion. Through an analysis of prominent cybercrime typologies including "digital arrest" scams, investment frauds, and financial cyber frauds, this paper identifies critical gaps in investigation capacity, judicial responsiveness, and victim protection mechanisms. The paper proposes that a rights-based approach to cybercrime regulation, integrating data protection, privacy safeguards, and victim-centered remedies, is essential to address vulnerabilities while maintaining democratic freedoms.

Keywords:*cybercrime, white-collar crime, human rights, digital fraud, India, victim protection, digital justice*

[1]PG Student, LL.M. (Human Rights Law), School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University, Chennai.

[2]Assistant professor of Law, Department of criminal law and criminal justice administration, The Tamil Nadu Dr. Ambedkar Law university, Chennai.

© 2025 International Journal of Advanced Legal Research

1. Introduction

The digital transformation of India has been characterized as one of the most ambitious technological integration projects globally, with initiatives such as Digital India, Aadhaar-enabled payment systems, and Unified Payments Interface (UPI) facilitating unprecedented financial inclusion. Yet this same digital infrastructure has become the vector for increasingly sophisticated forms of white-collar crime. Between 2022 and 2024, cybersecurity incidents in India increased 120%, rising from 10.29 lakh incidents to 22.68 lakh incidents. The financial toll has been equally alarming: cyber frauds resulted in reported losses exceeding ₹36.45 lakh on the National Cyber Crime Reporting Portal (NCRP) as of February 2025, with projected annual losses estimated to exceed ₹1.2 lakh crore (0.7% of India's GDP) in 2025.

The contemporary manifestation of cybercrime in India presents a qualitatively distinct phenomenon from traditional white-collar crime. It operates at the intersection of technological sophistication, transnational criminal networks, and psychological manipulation, creating what scholars have termed "digital tradecraft." Particularly alarming is the emergence of "digital arrest" scams, wherein fraudsters impersonate law enforcement officers through digital means, extorting approximately ₹3,000 crore from Indian citizens, predominantly seniors, before the Supreme Court's recent intervention.

This paper interrogates the relationship between the digital transformation of India's economy and the expansion of cybercriminal enterprise, specifically examining how existing legal, institutional, and governance frameworks fail to adequately protect fundamental human rights in this context. The central hypothesis guiding this inquiry is that the lacunae in India's cybercrime regulation create systematic vulnerabilities that transform cybercriminal activity from a discrete criminal phenomenon into a vehicle for widespread human rights violations, including threats to dignity, privacy, property rights, and access to justice.

2. Literature Review

2.1 Conceptualizing White-Collar Crime in the Digital Age

The foundational definition of white-collar crime is originating from Sutherland's 1939 conceptualization; it emphasized crimes committed by persons of respectability and high social

© 2025 International Journal of Advanced Legal Research

status in the course of their occupation. However, the contemporary scholarship has expanded this definition to encompass a broader array of non-violent financial crimes committed through abuse of organizational position or technological systems. The digital turn in white-collar criminality represents not merely a technological reframing of traditional crimes but a fundamental reconstitution of criminal capability, scale and geographic boundedness.

Becker and Stigler's seminal work on criminal penalties established that rational actors engage in crime when expected returns exceed legal sanctions discounted by apprehension probability. In the cybercrime context, this economic model proves inadequately predictive because (i) international jurisdictional fragmentation exponentially reduces apprehension probability, (ii) anonymity technologies (cryptocurrency, VPNs, mixing services) obscure criminal profits and (iii) transnational safe havens create de facto immunity zones.

Recent Indian scholarship has identified specific typologies of digital white-collar crime: insider trading through information asymmetry exploitation, data theft and sale.Cryptocurrencywas enabled money laundering and Ponzi schemes utilizing fintech platforms. The 2025 anti-fraud survey documented that phishing, investment scams and digital arrest frauds represent the three dominant categories, accounting for approximately 67% of reported incidents.

2.2 Human Rights Frameworks and Cybercrime Victimization

The intersection of cybercrime and human rights has emerged as an underdeveloped area within Indian legal scholarship, despite its critical significance. The International Covenant on Civil and Political Rights (ICCPR), to which India is a signatory, guarantees rights to life, liberty, dignity and protection against arbitrary interference with privacy. Yet existing Indian jurisprudence has largely compartmentalized cybercrime within the criminal law domain rather than situating it within human rights mediums.

The Supreme Court's recognition in *K.S. Puttaswamy v. Union of India* (2017) of privacy as a fundamental right under Article 21 of the Indian Constitution established crucial doctrinal foundations. However, subsequent jurisprudence has not adequately extended this protective framework to cybercrime victims, who experience simultaneous violations of privacy (data breaches), property (financial theft), and dignity (psychological manipulation).

© 2025 International Journal of Advanced Legal Research

Sinha's empirical research on cybercrime victimization in India reveals a critical gap between nominal rights recognition and lived experience. Victims frequently experience secondary victimization through investigative processes, victim-blaming discourse, and inadequate remedial mechanisms. Qualitative interviews documented that 73% of cyber fraud victims reported psychological trauma equivalent to violent crime victimization, yet received substantively inferior legal support.

2.3 Institutional and Legal Framework Analysis

India's primary cybercrime statute, the Information Technology (IT) Act, 2000 amended through the Information Technology (Amendment) Act, 2008 creates a framework primarily oriented toward data protection and computer system integrity rather than financial fraud prevention. Sections 66 and 66B address computer fraud and unauthorized access, but these provisions demonstrate significant interpretive limitations when applied to sophisticated cyber frauds involving multiple jurisdictions, technologies, and psychological dimensions.

The Indian Penal Code (IPC) sections addressing fraud (Section 420, criminal breach of trust) predate digital technology and require substantial judicial interpretation to apply meaningfully. The result is a legal framework characterized by doctrinal gaps, interpretive ambiguity, and institutional fragmentation.

Recent institutional responses provide partial counterweights to these legal deficiencies. The National Crime Records Bureau (NCRB) reported a 31.2% increase in registered cybercrime offenses between 2022 and 2023. The establishment of the Indian Cybercrime Coordination Center (I4C) and the National Cyber Crime Reporting Portal represent administrative innovations aimed at improving detection and victim support. However, these mechanisms remain underfunded relative to crime volume and operate within existing legal constraints.

Importantly, internet shutdowns-employed in response to cybercrime concerns in 80+ instances during 2023-create paradoxical human rights violations wherein the remedy (connectivity disruption) produces rights violations as severe as the disease (crime prevention).

© 2025 International Journal of Advanced Legal Research

2.4 Transnational Dimensions and Criminal Networks

A critical feature of contemporary Indian cybercrime is its transnational character. Over 50% of cyber frauds targeting Indians originate from Southeast Asian countries, particularly Cambodia, Myanmar, Vietnam, Laos and Thailand, operated from high-security compounds allegedly run by Chinese handlers. Indian intelligence has identified 45 scam centers in Cambodia alone, 5 in Laos and 1 in Myanmar.

This transnational infrastructure recruit's Indian nationals through fraudulent job offers, trafficking them through Dubai, China and Thailand to operate from foreign-based scam centers. Recruitment agents operate across Indian states including Maharashtra, Tamil Nadu, Jammu & Kashmir, Uttar Pradesh and Delhi, creating a domestic-transnational criminal network that frustrates traditional law enforcement models oriented toward territorial jurisdiction.

Castells' network society theory provides analytical utility here: these criminal enterprises operate as reterritorialized, horizontally-coordinated networks exploiting information asymmetries rather than as hierarchically-structured organizations. Disruption through conventional law enforcement targeting requires simultaneous action across multiple jurisdictions-a capacity India lacks.

2.5 Socio-Economic Dimensions of Vulnerability

Demographic analysis reveals that cyber fraud victimization concentrates among economically vulnerable populations: senior citizens, women, small business operators and lower-income earners investing savings in fraudulent schemes. The NITI Aayog has documented that societal shame surrounding victimization produces severe underreporting, with estimates suggesting 70-85% of victims never report, creating dark figures that obstruct both policy formulation and institutional response.

This demographic concentration intersects with structural inequality, as vulnerable populations often lack digital literacy and awareness of security best practices, yet occupy positions of economic desperation that render them susceptible to investment-based fraud.

© 2025 International Journal of Advanced Legal Research

3. Hypothesis

The legal, institutional, and governance frameworks regulating cybercrime in India are structurally inadequate to protect fundamental human rights, resulting in systematic vulnerabilities that enable cybercriminals to violate rights to property, privacy, dignity and access to justice simultaneously.

The digital transformation of economic infrastructure-while generating significant benefits-has created asymmetries of power, information and capability that current regulatory mechanisms cannot equilibrate, producing a rights deficit that extends beyond individual victimization to systemic threats to rule of law and democratic legitimacy.

4. Research Questions

1. What specific gaps exist between the formal legal framework governing cybercrime (IT Act, 2000; IPC provisions) and the substantive regulatory requirements necessary to prevent digital white-collar crime?
2. How do existing investigative and prosecution mechanisms fail to adequately address cybercriminal activity, particularly transnational dimensions?
3. What human rights dimensions of cybercrime victimization remain inadequately protected under existing law?
4. How do internet shutdowns and surveillance expansion-employed ostensibly as cybercrime prevention measures-themselves constitute human rights violations?
5. What institutional capacities require development to enable rights-respecting, effective cybercrime regulation?

5. The Digital Transformation of White-Collar Crime in India

5.1 Typologies of Cyber Fraud

Contemporary cyber frauds targeting Indian populations exhibit distinct morphologies:

© 2025 International Journal of Advanced Legal Research

A. Digital Arrest Scams: Fraudsters impersonate Central Bureau of Investigation (CBI), Income Tax Department or other law enforcement officials through WhatsApp, Telegram, or spoofed phone calls, falsely claiming outstanding legal liabilities and threatening arrest unless immediate payments transfer to designated accounts.[3] The Supreme Court's December 2025 intervention revealed that this single fraud typology generated ₹3,000 crore in reported losses, predominantly from senior citizens.[4]

B. Investment Frauds: Fake trading platforms, cryptocurrency schemes and Ponzi structures exploit investment aspirations through social media marketing and personalized outreach, promising unrealistic returns. The Mumbai Police documented 286 such cases in the first half of 2025 alone.[5]

C. Financial Cyber Frauds: Unauthorized account access, fake banking interfaces and UPI-based frauds exploit the integration of digital payment systems without corresponding security infrastructure updates. Credit card fraud, online banking scams and phishing represent dominant subcategories.

D. Job Fraud: Fake recruitment offers, particularly targeting youth, lure victims into paying processing fees or "training costs" for nonexistent positions or recruit them into transnational scam centers.

E. Task-Based and Gig-Economy Frauds: Platforms promising compensation for data entry, survey completion or social media engagement extract personal information or demand deposits before disappearing.

5.2 Scale and Economic Impact

The quantitative magnitude of cybercrime warrants emphasis. The reported statistics significantly understate actual impact:

[3] *Digital Arrest Scams: Modus Operandi and Institutional Response*, Drishti IAS (December 2, 2025). The fraud typically involves multiple contact points through WhatsApp, Telegram, or spoofed phone numbers, with fraudsters claiming connection to central law enforcement agencies.

[4] *Supreme Court Authorizes CBI to Investigate Digital Arrest Scams*, 2025 (December 1 order authorizing pan-India CBI investigation); victims predominantly senior citizens reportedly lost ₹3,000 crore in aggregate.

[5] Mumbai Police, Economic Offences Wing, White Collar Crime Statistics, First Half 2025 (June 2025).

© 2025 International Journal of Advanced Legal Research

- Registered incidents: 22.68 lakh (2024) vs. 10.29 lakh (2022)-120% increase in two years[6]
- Financial losses: ₹36.45 lakh reported on NCRP (Feb 2025); ₹120 crore in first nine months of 2024[7]
- Projected annual losses: ₹1.2 lakh crore (0.7% of GDP) in 2025[8]
- Digital arrest scam losses alone: ₹3,000 crore (concentrated in 2024-2025)[9]
- Estimated actual losses (accounting for underreporting): ₹3.5-4.5 lakh crore annually[10]

These figures reflect not merely individual financial loss but systemic economic disruption, reduced consumer confidence in digital payments, and erosion of trust in institutional systems.

5.3 Technological Sophistication and Criminal Innovation

Contemporary Indian cybercriminals deploy technological sophistication exceeding many institutional defensive capacities:

- Deepfake technology enabling video impersonation of government officials
- Cryptocurrency and blockchain-based money laundering obscuring transaction trails
- Distributed command-and-control infrastructure across multiple jurisdictions
- Advanced phishing utilizing social engineering and OSINT (open-source intelligence) collection
- Reverse proxy and VPN infrastructure enabling anonymity preservation

[6] Press Information Bureau, Curbing Cyber Frauds in Digital India (April 30, 2025).
[7]National Cyber Crime Reporting Portal, Dashboard Statistics (February 2025); ₹120 crore figure represents first nine months of 2024.
[8]Drishti IAS, Rising Cyber Frauds in India (July 18, 2025) (citing I4C projections); the ₹1.2 lakh crore figure represents 0.7% of India's 2024-25 estimated GDP.
[9]*Supreme Court Authorizes CBI to Investigate Digital Arrest Scams*, 2025 (December 1 order); the ₹3,000 crore refers to losses concentrated in digital arrest scams across 2024-2025 period.
[10]This estimation derives from NITI Aayog analysis suggesting actual victim pool exceeds reported pool by 3-4 times; if 15-25% of victims report, implied actual losses approach ₹3.5-4.5 lakh crore.

© 2025 International Journal of Advanced Legal Research

The Central Bureau of Investigation documented that digital tradecraft and the sophisticated use of digital tools to evade detectionhas become the baseline operational standard rather than exceptional practice.

6. Human Rights Vulnerabilities and Legal Gaps

6.1 Privacy and Data Protection

The Information Technology Act, 2000 provides limited data protection mechanisms, primarily addressing unauthorized access (Section 72). However, India lacks comprehensive data protection law equivalent to the EU's General Data Protection Regulation or California Consumer Privacy Act.[11] The Personal Data Protection Bill (2023), though significant, remains under legislative consideration and does not address criminal liability for data misuse in cybercrime contexts.

Vulnerabilities include:

Data breaches affecting millions (Aadhaar, voter databases, tax records) occur regularly without meaningful criminal consequences[12]

- No statutory right to notification following data breaches[13]
- Limited remedial mechanisms for victims of data misuse[14]
- Inadequate sectoral regulation of financial services, healthcare and government data[15]

This privacy deficit enables the initial data aggregation and targeting that makes cyber frauds effective.

[11]General Data Protection Regulation (GDPR), Regulation 2016/679, 2016 O.J. (L 119) (EU); California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.100 et seq. (2018); India's Personal Data Protection Bill, 2023 remains under legislative consideration and does not incorporate criminal fraud liability provisions

[12] Aadhaar database breaches in 2017-2018 affected over 1 billion individuals; voter database breaches reported in multiple states; tax record breaches documented in 2023.

[13] IT Act, 2000 lacks mandatory breach notification requirements equivalent to GDPR or CCPA.

[14] Remedial mechanisms limited to IPC Section 405 (criminal breach of trust) or IT Act civil provisions; aggregate remedies inadequate for mass victimization.

[15] Banking Regulation Act, 1949 provides limited data protection specifics; health information data regulation through HIPAA-equivalent absent.

© 2025 International Journal of Advanced Legal Research

6.2 Property Rights and Financial Access

Article 19 and 300A of the Indian Constitution guarantee property rights; yet cybercrime creates situations were financial fraud results in property loss without corresponding remedy mechanisms. Victims lack:

- Criminal compensation provisions specifically addressing cyber fraud[16]
- Civil remedies adequate to compensate aggregate losses across thousands of victims[17]
- Expedited asset recovery procedures accounting for rapid cryptocurrency conversion
- Victim restitution funds analogous to victim compensation schemes in other jurisdictions[18]

6.3 Dignity and Psychological Trauma

Human rights jurisprudence recognizes dignity as a fundamental right encompassing freedom from humiliation, psychological harm and coercion.[19] Cyber frauds, particularly digital arrest scams, inflict dignitary harms through:

- Psychological coercion and threat simulation
- Social stigma surrounding victimization that prevents help-seeking[20]
- Institutional victim-blaming in investigation and prosecution processes
- Inadequate victim support and counseling services[21]

[16] Criminal Procedure Code, 1973 provides victim compensation provisions under Sections 357-357A; however, provisions historically underutilized in cybercrime contexts and provide inadequate quantum.
[17] Civil remedies under tort law provide theoretical basis for damages actions; however, proof requirements and collective action barriers limit practical effectiveness.
[18] Victim compensation funds exist in some U.S. jurisdictions but remain absent in Indian framework; Crime Victim Compensation Board model not replicated in India.
[19] Article 21, Indian Constitution; *K.S. Puttaswamy v. Union of India,* AIR 2017 SC 4161 (recognizing dignity as core component of fundamental right to life).
[20] NITI Aayog study documents that 78% of cyber fraud victims experience societal stigma hindering victim disclosure and help-seeking.
[21] Helpline 1930 provides initial assistance; however, follow-up psychological support services minimal and geographically limited

© 2025 International Journal of Advanced Legal Research

Qualitative research documents that cyber fraud victims experience psychological sequelae equivalent to violent crime victimization, including PTSD, depression and suicidality, yet receive negligible institutional support.[22]

6.4 Access to Justice and Remedy

The principle of access to justice, recognized in *Hussainara Khatoon v. Home Secretary* and subsequent cases,[23] requires meaningful opportunity to pursue grievances before impartial tribunals. Cybercrime victimization frustrates this principle through:

- Transnational jurisdiction barriers preventing prosecution
- Technical complexity requiring specialized forensic expertise absent in many police departments
- Evidentiary challenges arising from digital format and chain-of-custody requirements
- Institutional capacity deficits resulting in 2-3yearinvestigation timelines for complex cases
- Limited victim participation in investigation and prosecution processes

The result is functionally diminished access to justice for cyber fraud victims relative to traditional crime victims.

7. Institutional and Legal Framework Analysis

7.1 Statutory Limitations

The IT Act, 2000 addresses computer fraud primarily through Sections 66 and 66B. Section 66 imposes liability for persons who "access or cause to be accessed" computer resources "with the intent to cause wrongful loss or gain."[24] However, interpretation has concentrated on

[22] Qualitative research by Arpita Sinha documents PTSD, depression, and suicidality in cyber fraud victims at rates equivalent to violent crime victims; institutional mental health support dramatically inferior to violent crime victim support.
[23] *Hussainara Khatoon v. Home Secretary, State of Bihar*, AIR 1979 SC 1369 (establishing access to justice as fundamental right component).
[24] Information Technology Act, 2000 § 66 (establishing liability for intentional unauthorized access causing wrongful loss or gain).

© 2025 International Journal of Advanced Legal Research

unauthorized system access rather than fraud perpetrated through authorized access using stolen credentials.

Section 66C (identity theft) requires proof of "fraudulent or dishonest use" but demonstrates interpretive narrowness when applied to sophisticated identity spoofing or synthetic identity creation. Similarly, Section 66D (cheating by impersonation) requires proof of intent to cause wrongful loss, which prosecutions frequently fail to establish beyond reasonable doubt.

IPC Sections 420 (cheating) and 405 (criminal breach of trust) predate digital technology. While courts have applied these provisions to cybercrime contexts,[25] the doctrinal gap between the statutory language and contemporary criminal sophistication creates predictable acquittals and inconsistent jurisprudence.

7.2 Investigative Capacity Deficits

The NCRB (2023) identified critical investigative limitations:

- Average investigation timeline: 24-36 months for complex cyber fraud cases[26]
- Forensic expertise concentration in metropolitan areas; negligible capacity in smaller jurisdictions[27]
- Limited technical training for investigating officers, with 67% lacking formal digital forensics training[28]
- Cross-border collaboration mechanisms inadequate for transnational crime investigation[29]
- Chain-of-custody and digital evidence preservation protocols inconsistently applied[30]

[25]Courts apply IPC § 420 and § 405 to cybercrime contexts through interpretive extension; examples include cases addressing online trading fraud and investment scheme prosecution
[26] NCRB, Crime in India 2023 (documenting investigation timelines).
[27] Forensic expertise concentration in Delhi, Mumbai, Bangalore, Hyderabad; significantly limited capacity in tier-2 and tier-3 cities.
[28] NCRB digital forensics training survey (2023) documents that 67% of investigating officers lack formal training; 43% lack practical experience with digital evidence collection.
[29] INTERPOL coordination and bilateral law enforcement agreements provide partial mechanisms; however, institutional barriers and diplomatic complications frustrate effective collaboration.
[30] Digital evidence chain-of-custody requirements inconsistently applied; forensic imaging protocols vary across jurisdictions; evidence integrity occasionally compromised through improper handling.

© 2025 International Journal of Advanced Legal Research

The CBI's 2025 report documented that investigative delays frequently exceed statutes of limitation, resulting in case closure without prosecution.

7.3 Judicial Response and Case Outcomes

Conviction rates in cybercrime prosecutions remain significantly lower than traditional crime convictions. The NCRB (2023) documented conviction rates of approximately 15-22% in cyber fraud cases compared to 45-50% in traditional property crimes.[31] Judicial complexities include:

- Technical evidence interpretation requiring specialized judicial education
- Evidentiary standards derived from analogue-era jurisprudence ill-suited to digital evidence
- Sentencing patterns failing to reflect crime severity and victim impact
- Limited precedential jurisprudence establishing consistent interpretive frameworks

7.4 Recent Institutional Innovations

The December 2025 Supreme Court directive represents a significant institutional innovation.[32] By authorizing the CBI to investigate digital arrest scams across state boundaries under Section 6 of the Delhi Special Police Establishment Act, the Court addressed jurisdictional fragmentation that previously enabled criminals to operate with impunity across state lines.[33]

Additional institutional developments include:

- **Indian Cybercrime Coordination Center (I4C):** Established 2023 to coordinate multi-agency response, though operating with limited resources relative to crime volume[34]

[31] NCRB, Crime in India 2023 (documenting cybercrime conviction rates of 15-22% compared to property crime conviction rates of 45-50%).
[32] *Supreme Court Authorizes CBI to Investigate Digital Arrest Scams*, 2025 (December 1 order).
[33] Section 6, Delhi Special Police Establishment Act, 1946 (empowering CBI to investigate offenses with written consent of state governments); Supreme Court directive authorizing CBI to investigate digital arrest scams across multiple states circumvents requirement by authorizing states to provide blanket consent for this crime typology.
[34] I4C established 2023; operates with staff of approximately 150-200 personnel; complaint volume in 2024-2025 exceeds institutional capacity.

© 2025 International Journal of Advanced Legal Research

- **National Cyber Crime Reporting Portal (NCRP):** Enables online reporting; cybercrime.gov.in processed 9.94 lakh complaints and prevented ₹3,431 crore in losses by November 2025[35]
- **Helpline 1930:** Provides immediate victim assistance and crime reporting; insufficient staffing relative to call volume[36]
- **Anti-spoofing Systems:** Blocking 9.42 lakh SIM cards and 2,63,348 IMEIs linked to fraud; administrative measure with limited predictive capacity[37]

However, these innovations operate within existing legal constraints and remain underfunded relative to crime scale.

8. Internet Shutdowns and Paradoxical Rights Violations

A particularly troubling institutional response to cybercrime involves internet shutdowns. Between 2022 and 2024, India issued over 80 internet shutdown orders, apparently to prevent cybercriminal coordination or maintain public order.[38] However, this remedy produces rights violations potentially exceeding the disease it purports to cure.

The Supreme Court in *Anuradha Bhasin v. Union of India* (2020) established that internet shutdowns require procedural safeguards: necessity, proportionality, limited scope and duration, and accountability mechanisms.[39]Yet subsequent shutdowns have regularly violated these safeguards, particularly in contexts of communal tension or protest.[40]

Human Rights Watch's 2023 analysis documented that broad shutdowns disproportionately harm economically vulnerable populations dependent on digital access for employment, government

[35] National Cyber Crime Reporting Portal, Operational Statistics (November 2025).
[36] Helpline 1930 operates with limited staff relative to call volume; many calls encounter busy signals or automated systems rather than trained counselors.
[37] Press Information Bureau, Curbing Cyber Frauds in Digital India (April 30, 2025).
[38] Access Now, India's Internet Shutdowns 2023 (June 2023); Software Freedom Law Centre, Internet Shutdowns in India, 2023.
[39]*Anuradha Bhasin v. Union of India*, AIR 2020 SC 1. The Supreme Court established requirements of: necessity (genuine public order threat), proportionality (minimal intrusion adequate to address threat), limitation (temporal and geographic scope minimized), and transparency/accountability
[40] Post-*Anuradha Bhasin*, shutdown orders have continued to occur without satisfying established safeguards; particularly problematic in contexts of communal tension, protest, or political demonstration.

© 2025 International Journal of Advanced Legal Research

services, and financial inclusion.[41] A shutdown preventing cybercriminal coordination simultaneously prevents:

- Access to government social protection programs[42]
- Gig economy employment opportunities[43]
- Medical and health services delivery
- Educational access in digital learning contexts
- Financial services and digital payments

This represents state-imposed human rights violation allegedly justified by cybercrime prevention-a problematic governance response.

9. Transnational Dimensions and Jurisdictional Challenges

9.1 Criminal Safe Havens and Prosecution Barriers

The transnational character of cybercrime networks frustrates India-centric law enforcement responses. Cambodia hosts 45 documented scam centers; Laos hosts 5; Myanmar hosts at least 1.[44]These facilities operate under state tolerance or protection, creating effective immunity zones for cybercriminals targeting India.

International cooperation mechanisms prove inadequate:

- Mutual Legal Assistance Treaty (MLAT) processes require 12-24 months
- Extradition treaties lack cybercrime-specific provisions
- Evidence gathering across jurisdictions faces evidentiary and technical barriers

[41] Human Rights Watch, 'No Internet Means No Work, No Pay, No Food': Internet Shutdowns Deny Access to Basic Rights in Digital India (June 2023).
[42] PMJDY (Pradhan Mantri Jan Dhan Yojana) account access, government subsidy distribution, welfare payment access all require internet connectivity.
[43] Gig economy workers (Ola, Uber, delivery platforms) lose income opportunity during shutdown periods; aggregate economic loss significant for low-income workers.
[44] Press Information Bureau, Cyber Frauds: Transnational Dimensions (April 30, 2025).

© 2025 International Journal of Advanced Legal Research

- No harmonized international criminal liability standards[45]

9.2 Domestic Trafficking and Forced Labor

A critical human rights dimension involves recruitment of Indian nationals for forced labor in transnational scam centers. The CBI's 2025 report documented systematic recruitment through fraudulent job offers in Maharashtra, Tamil Nadu, J&K, UP and Delhi.[46] Victims face:

- Document confiscation and debt bondage[47]
- Threats and violence preventing escape
- Forced participation in cybercrime, creating legal liability complications
- Trafficking victim classification and protection mechanisms inadequately applied to cybercrime victims[48]

This represents convergence between cybercrime and human trafficking-distinct human rights violations requiring integrated responses.

10. Recommendations and Toward a Rights-Based Cybercrime Framework

10.1 Legislative Reform

A. Comprehensive Cyber Fraud Act: India requires standalone legislation specifically addressing cyber fraud, distinguishing it from unauthorized computer access or data protection violations. Such legislation should incorporate:

- Explicit criminalization of sophisticated fraud techniques (phishing, identity spoofing, deepfake impersonation)[49]

[45] International cybercrime conventions (Budapest Convention on Cybercrime, 2001) provide partial harmonization; however, not all relevant nations parties to Convention (China, Cambodia, Myanmar, Laos not parties).
[46] CBI, Human Trafficking and Cybercrime Nexus (2025) (sealed report).
[47] Document confiscation and debt bondage (payment for transport, recruitment fees, "training" recouped through victim's criminal labor) constitute forced labor indicators.
[48] Trafficking victims entitled to protection under Immoral Traffic Prevention Act (ITPA), 1956 and Prevention of Trafficking of Persons (PTPP) Act, 2018; however, cybercrime victim-trafficking nexus not systematically recognized.
[49]Statutory criminalization of identity spoofing, deepfake creation and transmission for fraud purposes, phishing when combined with financial fraud intent would address gaps in existing IT Act § 66 and IPC § 420 provisions.

© 2025 International Journal of Advanced Legal Research

- Statutory liability for fraudulent use of authorized access[50]
- Sentencing guidelines accounting for victim impact and aggregate loss[51]
- Victim compensation provisions and restitution requirements
- International cooperation mechanisms and mutual legal assistance procedures[52]

B. Data Protection Legislation: Enactment of comprehensive data protection law integrating:

- Criminal liability for data misuse and unauthorized disclosure[53]
- Mandatory breach notification and victim compensation[54]
- Sectoral regulation with enhanced protections for financial and health data[55]
- Private rights of action for data breach victims[56]

C. Victim Rights Legislation: Dedicated victim protection statute providing:

- Counseling and psychological support services
- Civil cause of action for dignitary harm damages
- Victim compensation fund financed through criminal penalties
- Procedural protections against secondary victimization

10.2 Institutional Capacity Development

A. Specialized Investigative Units: Establishment of dedicated cybercrime investigation units at state and district levels with:

[50]Authorized access fraud involves legitimate system access credentials used fraudulently; existing IT Act § 66 requires "unauthorized access" making prosecution difficult when access authorized but use fraudulent.
[51] Sentencing guidelines accounting for victim count, aggregate financial loss, victim vulnerability, and psychological impact would rationalize sentencing and reflect crime severity.
[52] Specific provisions addressing MLAT procedures, extradition frameworks, mutual investigation protocols, evidence-sharing procedures would streamline international cooperation.
[53]Criminal liability for data misuse (unauthorized disclosure, sale, or fraudulent use) would extend liability beyond IPC § 405 (criminal breach of trust) to encompass data-specific harm.
[54] Mandatory notification requirements and victim compensation fund provisions modeled on GDPR/CCPA would create deterrence and victim remedy mechanisms.
[55] Financial sector data protection (banking, investment), health data protection, and government sensitive data (Aadhaar, tax, electoral) require enhanced sectoral regulation.
[56] Private rights of action (in tort/civil law) enable victims to pursue remedies without dependence on state prosecution; equivalent to EU GDPR private enforcement mechanisms.

© 2025 International Journal of Advanced Legal Research

- Mandatory digital forensics training for all investigating officers[57]
- Technical expertise through partnerships with technology sector professionals[58]
- Adequate budgeting for forensic tools and infrastructure[59]

B. Judicial Education: Judicial training programs addressing:

- Digital evidence admissibility and evaluation[60]
- Technical complexity and authentication procedures[61]
- Victim impact assessment in cybercrime contexts[62]

C. International Cooperation Mechanisms:

- Bilateral and multilateral law enforcement agreements[63]
- Joint task forces with international partners[64]
- Harmonized investigation standards and evidence-sharing protocols[65]

10.3 Rights-Protective Governance

A. Internet Shutdowns Regulation: Strict adherence to Supreme Court requirements in *Anuradha Bhasin*, including:

- Genuine necessity determinations with documented evidence[66]

[57] Mandatory digital forensics training for all investigating officers; specialized advanced training for dedicated cybercrime units.
[58] Public-private partnerships with technology companies enable secondment of technical expertise; contractor arrangements with forensic specialists supplement institutional capacity.
[59] Digital forensics laboratories, hardware/software infrastructure (write-blockers, analysis tools, servers), and ongoing maintenance represent substantial budgetary requirements inadequately provided in current allocations.
[60] Judicial education programs addressing digital evidence authentication, encryption cryptography basics, metadata analysis, and forensic tool reliability assessment.
[61] Training on chain-of-custody protocols for digital evidence, bit-level imaging requirements, and forensic integrity preservation.
[62] Judicial understanding of cybercrime victim impact (psychological trauma, financial loss, reputational harm) would inform more appropriate sentencing.
[63] Bilateral law enforcement cooperation agreements with Southeast Asian nations providing mutual investigation support, evidence access, and extradition frameworks.
[64] Joint task forces with U.S. FBI, Europol, INTERPOL, and bilateral partners would enable coordinated investigation of transnational cybercrime networks.
[65] Harmonized investigation standards, evidence preservation protocols, and evidence-sharing agreements would streamline international cooperation

© 2025 International Journal of Advanced Legal Research

- Temporal and geographic limitation to minimum required period and area[67]
- Independent judicial review before implementation[68]
- Accountability for unlawful shutdowns[69]

B. Privacy-by-Design Requirements: Integration of privacy principles into digital payment systems, fintech platforms, and government digital services through:

- Mandatory security audits and penetration testing[70]
- Data minimization principles limiting collection and retention[71]
- User authentication requirements and breach prevention standards[72]

C. Victim Support Systems: Comprehensive victim assistance including:

- 24/7 helplines with trained counselors[73]
- Emergency financial assistance for fraud victims experiencing hardship[74]
- Legal aid for pursuit of remedies[75]
- Integration with mental health services[76]

---

[66] Internet shutdowns require demonstrated necessity through documented evidence of imminent public order threat; generalized security concerns insufficient justification per *Anuradha Bhasin*.
[67] Shutdowns limited to minimum geographic area (district rather than state-wide) and minimum temporal duration (hours rather than days-weeks) required by proportionality principle.
[68] Independent judicial review (ideally Supreme Court or High Court) before shutdown implementation to ensure compliance with *Anuradha Bhasin* safeguards.
[69] Accountability for unlawful shutdowns through judicial damages proceedings and administrative action against ordering officials would create incentive compliance.
[70] Mandatory security audits, penetration testing, and vulnerability disclosure protocols for digital payment systems, fintech platforms, and government digital services would prevent initial fraud enablement.
[71] Data minimization (collection/retention only when necessary); purpose limitation (use only for stated purposes); encryption and technical safeguards.
[72] Multi-factor authentication requirements, behavioral biometrics, transaction verification protocols would prevent unauthorized account access.
[73] 24/7 helplines with trained trauma-informed counselors; regional language accessibility; integration with police reporting mechanisms.
[74] Emergency financial assistance for fraud victims experiencing acute hardship; coordination with civil society organizations.
[75] Legal aid for pursuit of civil remedies; assistance with MLAT proceedings and international cooperation.
[76] Integration with mental health services, trauma counselors, and psychological support; coordination with social welfare services.

© 2025 International Journal of Advanced Legal Research

11. Conclusion

The digital turn in white-collar crime represents not merely an evolution of traditional criminal techniques but a fundamental challenge to human rights protection in India's emerging digital economy. The proliferation of sophisticated cyber frauds, digital arrest scams, investment frauds, and transnational criminal networks has created a context wherein existing legal, institutional, and governance frameworks demonstrate systematic inadequacy.

The empirical evidence is unambiguous: cybersecurity incidents have increased 120% between 2022 and 2024; financial losses exceed ₹1.2 lakh crore annually; digital arrest scams alone generated ₹3,000 crore in reported losses; and over 50% of cyber frauds targeting Indians originate from Southeast Asian safe havens beyond effective jurisdictional reach.

Yet these quantitative dimensions obscure the profound human rights implications. Cyber fraud victims simultaneously experience violations of privacy through data breaches, property rights through financial theft, dignity through psychological manipulation and social stigma, and access to justice through transnational jurisdiction barriers. Institutional responses, including internet shutdowns, frequently perpetrate human rights violations as severe as the crimes they purport to prevent.

The central proposition of this paper-that cybercrime regulation in India operates within a structural human rights deficit-emerges clearly from this analysis. Resolution requires integrated action across legislative, institutional, and governance domains:

- **Legislatively:** Enactment of comprehensive cyber fraud statutes, data protection legislation, and victim rights frameworks
- **Institutionally:** Development of specialized investigative capacity, forensic expertise, and international cooperation mechanisms
- **Governance-wise:** Protection of internet access rights, victim-centered policy formulation, and accountability for state responses

The digital transformation of India's economy represents significant achievement, yet without corresponding human rights protections, it creates asymmetries of vulnerability and power that

© 2025 International Journal of Advanced Legal Research

undermine rule of law and democratic legitimacy. A rights-based cybercrime framework-one integrating victim protection, privacy preservation, and proportionate remedies-is not merely desirable but essential to ensure that digital inclusion becomes genuine inclusion rather than engineered vulnerability.

The Supreme Court's recent actions provide modest encouragement that institutional awareness of cybercrime severity is increasing. However, without legislative reform addressing doctrinal gaps, without institutional capacity development enabling effective investigation and prosecution, and without governance frameworks prioritizing human rights over surveillance, India will continue to witness the tragic contradiction: extraordinary technological achievement accompanied by extraordinary technological victimization.

© 2025 International Journal of Advanced Legal Research