WRONGFUL IMPLICATION OF INNOCENT PERSONS IN CYBERCRIME CASES:

A Study of Digital Identity Misuse and Investigative Lapses in Light of Article 21 of the Constitution of India

ABSTRACT

Digital technology's rapid proliferation across India has generated a troubling pattern: innocent individuals are routinely prosecuted as cybercriminals as a consequence of digital identity misuse and systemic investigative deficiencies. This paper examines how victims of IP address spoofing, SIM cloning, phishing, and account hijacking come to bear criminal liability for offences perpetrated by others using their stolen digital identities. Grounded in the constitutional guarantee of personal liberty under Article 21, this study critically evaluates the legislative gaps within the Information Technology Act, 2000 (IT Act), the IT (Amendment) Act, 2008, and the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), which together render innocent persons vulnerable to wrongful prosecution. Through analysis of judicial decisions and documented investigative failures, the paper demonstrates that the existing legal framework inadequately addresses the forensic complexities of digital attribution. Structural reform is urgently required, encompassing mandatory digital forensic standards, statutory safeguards against premature arrest, independent oversight of cyber investigations, and legislative recognition of digital identity theft as a discrete serious offence. Without such reform, the constitutional promise of Article 21 remains unrealised for those caught in the failures of the digital criminal justice system.

Keywords: Article 21, cybercrime, digital identity theft, wrongful prosecution, forensic lapses, IT Act, criminal justice reform, Bharatiya Nagarik Suraksha Sanhita.

I. INTRODUCTION

India's digital revolution has transformed the landscape of crime and criminal justice alike. With over 900 million internet users and one of the fastest-growing digital economies globally, the country has witnessed a steep surge in cybercrime. According to the National Crime Records Bureau (NCRB), cybercrime incidents increased by more than twenty-four percent in 2022, with upwards of 65,893 cases registered under the IT Act and allied provisions.[1] Embedded within these figures is a distressing reality: a significant proportion of those implicated are not perpetrators but victims — persons whose digital identities have been stolen, cloned, or falsely attributed by the actual offender.

Wrongful implication in cybercrime cases constitutes one of the gravest failures of contemporary criminal justice. Unlike traditional crime, where physical evidence and witness testimony anchor attribution, cybercrime investigation depends almost entirely on digital evidence — IP addresses, device identifiers, metadata, and authentication logs — all of which are susceptible to manipulation and misattribution. A skilled offender can route criminal activity through an unsuspecting person's IP address, clone a SIM card to execute financial fraud, or exploit stolen credentials to commit offences that law enforcement will then wrongly attribute to the identity holder.

The consequences for the wrongly accused are severe and often permanent. Article 21 of the Constitution of India guarantees that no person shall be deprived of life or personal liberty except in accordance with a procedure established by law. The Supreme Court of India has interpreted this provision expansively to include the rights to dignity, privacy, reputation, and a fair trial.[2] When an innocent person is arrested, publicly named as a cybercriminal, dismissed from employment, and subjected to protracted criminal proceedings — all on the basis of a defective IP lookup or inadequate forensic investigation — each of these rights stands violated. The state, paradoxically, becomes the instrument of harm against the very citizen it is constitutionally bound to protect.

---

[1] Nat'l Crime Recs. Bureau, Crime in India 2022, Ministry of Home Affs., Gov't of India 47 (2023).
[2] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 [hereinafter *Puttaswamy*].

This paper proceeds in the following order. Part II contextualises the nature of digital identity and its mechanisms of misuse. Part III analyses structural weaknesses in India's investigative and legal framework. Part IV examines the constitutional framework under Article 21. Part V identifies legislative gaps in existing statutes. Part VI analyses relevant judicial decisions. Part VII surveys comparative international frameworks. Part VIII proposes a set of targeted reforms, and Part IX concludes.

II. DIGITAL IDENTITY AND THE MECHANISMS OF ITS MISUSE

A. The Concept of Digital Identity

Digital identity comprises the aggregate of information that identifies a person or entity within the online environment: IP addresses, email addresses, device identifiers (MAC addresses and IMEI numbers), social media accounts, digital certificates, biometric data, and authentication credentials.[3] In cybercrime investigation, digital identity functions as the primary basis for attribution — it is the trail connecting a criminal act to its alleged perpetrator. The reliability of that attribution depends entirely on the integrity of the underlying identity, which cannot be assumed.

Indian law has not yet developed a comprehensive statutory definition of digital identity. The IT Act addresses discrete aspects — digital signatures under Section 3, electronic records under Section 4, and unauthorised access under Section 43 — but articulates no holistic legal framework for digital identity protection. The Digital Personal Data Protection Act, 2023 (DPDPA) marks a step forward in recognising individual data rights but falls short of directly addressing the forensic misattribution of digital identity in criminal proceedings.

B. Principal Mechanisms of Digital Identity Misuse

1. IP Address Spoofing and Proxy Routing

[3]Ravi Shankar Prasad, Digital Identity and Governance Framework, NASSCOM Policy Report 12 (2021).

Internet Protocol addresses are numerical labels assigned to network-connected devices. Law enforcement agencies routinely rely upon IP address logs as the initial step in identifying cybercrime suspects. However, IP addresses can be manipulated through Virtual Private Networks (VPNs), Tor networks, proxy servers, and botnet infrastructure, enabling offenders to route criminal activity through the IP address of an innocent third party.[4] Where investigators retrieve IP logs without further analysis — without examining metadata layers, device fingerprints, or network topology — an innocent subscriber whose IP address served merely as a conduit becomes the suspect.

A Lucknow case from 2021 illustrates this pattern. A school teacher was arrested by Uttar Pradesh Police on charges of transmitting obscene content online, solely on the basis of IP records obtained from an Internet Service Provider. The actual offender had routed traffic through the teacher's broadband connection via a compromised router. High Court intervention and an independent forensic audit established that the device used for transmission had never been in the teacher's possession.[5]

2. SIM Card Cloning and Mobile Identity Theft

SIM card cloning involves duplicating a subscriber's SIM to intercept communications and conduct fraudulent transactions under the subscriber's mobile identity. In India, mobile numbers are linked to Aadhaar, bank accounts, and UPI payment systems, making mobile identity theft a gateway to a wide range of financial and communicative offences. When fraud is committed using a cloned SIM, the subscriber whose number was cloned becomes the primary suspect in the digital trail — unless law enforcement possesses both the capability and the motivation to investigate further.

Sections 66C and 66D of the IT Act criminalise identity theft and cheating by impersonation using computer resources respectively. These provisions are, however, primarily invoked against perpetrators once apprehended, rather than to exonerate victims already wrongly implicated. The

[4]Internet Security Alliance, Cyber Threats and Digital Identity Misuse: A Global Overview 34 (2022).

[5]Lucknow Teacher Wrongly Arrested for Cybercrime Based on IP Address, The Wire (Mar. 15, 2021), https://thewire.in/law/lucknow-teacher-cybercrime-ip-address (last visited Apr. 20, 2025).

absence of a mandatory forensic verification step — requiring investigators to confirm exclusive possession and use before arrest — creates a structural vulnerability that recurrently harms innocent persons.

3. Phishing, Account Hijacking, and Credential Theft

Phishing involves the use of deceptive communications to induce users to surrender their login credentials, enabling attackers to operate under the victim's digital identity. Account hijacking through phishing has been used to publish unlawful content, commit financial fraud, and transmit threats — all appearing to originate from the registered account holder. Law enforcement, upon receiving complaints, frequently obtains activity logs from platforms and proceeds against the registered user without considering the possibility of account compromise.

This investigative shortcut violates the foundational precept of criminal law that liability must be personal and must rest on culpable individual conduct. The Supreme Court affirmed in *K.S. Puttaswamy v. Union of India*[6] that informational privacy is a fundamental right and that any state action threatening a person's data must be proportionate and procedurally fair. Treating account ownership as conclusive evidence of criminal activity — without adequate forensic investigation — is precisely the kind of disproportionate and arbitrary state conduct that Article 21 prohibits.

4. Deepfakes and Synthetic Digital Identity

An increasingly pernicious form of digital identity misuse is the creation of synthetic content — deepfakes — that places an innocent person's face, voice, or digital likeness in criminal or defamatory contexts. Artificial intelligence-powered deepfake technology can produce highly convincing fabricated videos and audio recordings appearing to show a person committing an offence. Indian courts and law enforcement agencies are only beginning to grapple with this challenge, and no specific statutory provision yet addresses deepfake-based identity misuse in the context of wrongful criminal implication.

[6]Puttaswamy, *supra* note 2.

III. INVESTIGATIVE LAPSES: STRUCTURAL FAILURES IN INDIA'S CYBERCRIME ENFORCEMENT

A. Inadequate Forensic Capacity

The most fundamental structural failure in India's cybercrime enforcement apparatus is the acute shortage of trained digital forensic personnel. As of 2023, India had only approximately one thousand certified digital forensic examiners across all law enforcement agencies — a ratio starkly insufficient relative to the volume and complexity of cybercrime cases.[7] Most police stations, particularly at district and sub-divisional levels, lack access to forensic cyber laboratories. Investigations are therefore conducted by officers who, at best, possess a rudimentary understanding of digital evidence and, at worst, display a dangerously overconfident familiarity with surface-level tools such as IP lookup services.

The consequence of this forensic deficit is well-documented. Officers frequently rely on first-order digital evidence — an IP address, a phone number, a registered email — without conducting the deeper analysis that would reveal whether the identified device was actually used for the alleged offence, whether the account was accessed by someone other than the registered user, or whether the digital trail had been deliberately manipulated. This shallow investigative methodology creates a direct pathway from digital identity to wrongful arrest.

B. Over-Reliance on Subscriber Data Without Corroboration

Law enforcement agencies routinely obtain subscriber data from Internet Service Providers and telecom operators under Sections 94 to 99 of the BNSS and Section 69B of the IT Act. This data identifies the registered subscriber of a particular IP address or mobile number at the material time.

[7] Ctr. for Internet & Soc'y, State of Digital Forensics in India 8 (2023).

The critical error lies in equating subscriber identity with offender identity — a conflation that is forensically indefensible.

A registered subscriber is merely a contractual party to a service agreement. Multiple family members may share a broadband connection; a mobile phone may be borrowed, stolen, or remotely compromised. Without device-level forensic analysis — examination of the actual device for logs, browser history, metadata, authentication records, and location data — subscriber identity alone is insufficient to establish personal culpability. Yet the arrest of subscribers on the basis of IP logs alone remains a routine practice.

C. Absence of Enforceable Digital Evidence Standards

India has no mandatory, legally enforceable standard for the collection, preservation, and analysis of digital evidence in cybercrime investigations. The Cyber Crime Investigation Manual issued by the Ministry of Home Affairs provides guidelines, but these are advisory rather than statutory. The result is significant variation in investigative quality, with many investigations proceeding without basic forensic principles such as chain of custody documentation, hash verification, and the use of write-blocking tools to prevent alteration of original evidence.

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) — carrying forward Section 65B of the Indian Evidence Act, 1872 — requires certification to authenticate electronic records produced as evidence. The Supreme Court in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[8] held that this requirement is mandatory and non-waivable. While this decision strengthens the evidentiary standard at trial, it does not correct the investigative process upstream, where defective digital evidence is gathered and used to justify arrest and detention long before any judicial scrutiny is applied.

D. Premature Arrest and Misuse of Custodial Powers

[8] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

One of the most constitutionally consequential investigative lapses is the tendency to arrest cybercrime suspects at the earliest opportunity, before investigations are complete and before the accused have had any opportunity to establish their innocence. The Supreme Court's directions in *Arnesh Kumar v. State of Bihar*[9] require police officers to satisfy themselves of the necessity of arrest before proceeding, and Magistrates to apply independent consideration before remanding accused persons to custody. These guidelines are routinely disregarded in cybercrime cases, where technical complexity is used to justify extended custodial interrogation that amounts to punishment before verdict.

IV. CONSTITUTIONAL FRAMEWORK: ARTICLE 21 AND THE RIGHTS OF THE WRONGLY ACCUSED

A. The Expansive Scope of Article 21

Article 21 of the Constitution of India provides that no person shall be deprived of life or personal liberty except according to procedure established by law. Decades of judicial interpretation have transformed this provision into the most expansive guarantee in the constitutional order. The Supreme Court has recognised that Article 21 encompasses not merely freedom from arbitrary detention, but a constellation of substantive rights including the right to dignity,[10] privacy,[11] reputation,[12] a fair trial,[13] and compensation for state-inflicted injury.[14]

Each of these rights is directly engaged when an innocent person is wrongly implicated in a cybercrime case. Personal liberty is violated by unlawful arrest. Dignity is violated by public identification as a criminal. Privacy is violated by the unregulated seizure and examination of personal devices and data. Reputation is violated by the social and professional consequences of a

[9]Arnesh Kumar v. State of Bihar, (2014) 8 SCC 273.
[10]Francis Coralie Mullin v. Adm'r, Union Territory of Delhi, (1981) 1 SCC 608.
[11]Puttaswamy, *supra* note 2.
[12]Kiran Bedi v. Comm. of Inquiry, (1989) 1 SCC 542.
[13]Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[14]Nilabati Behera v. State of Orissa, (1993) 2 SCC 746.

criminal accusation. And the right to a fair trial is undermined when the investigative foundation of the case is structurally defective.

B. The Right to Privacy in the Digital Age

The nine-judge Constitution Bench in *Justice K.S. Puttaswamy (Retd.) v. Union of India*[15] held unequivocally that privacy is a fundamental right under Article 21, encompassing informational privacy — the right of persons to control information about themselves. In the cybercrime investigation context, this right is implicated when law enforcement accesses digital communications without adequate legal authority, when subscriber data is disclosed to investigators without judicial oversight, and when personal devices are seized and examined without proportionate justification.

The *Puttaswamy* framework requires that any infringement of privacy satisfy a tripartite test: legality (authorisation by law), legitimate aim (a pressing public purpose), and proportionality (the least intrusive means of achieving that aim). Applied to cybercrime investigations, this demands that investigative techniques — data collection, device seizure, digital surveillance — be proportionate to the offence under investigation and accompanied by adequate procedural safeguards. The current framework falls short of this standard in critical respects.

C. The Right Against Arbitrary Arrest and Detention

Article 21, read with Article 22, guarantees that no person may be arrested without a valid legal basis and that every arrested person must be produced before a Magistrate within twenty-four hours. The Supreme Court in *D.K. Basu v. State of West Bengal*[16] prescribed comprehensive guidelines for lawful arrest, requiring documentation, communication of grounds, and notification of family members. In cybercrime cases, where the evidentiary basis for arrest is technical and opaque, the accused frequently lacks any immediate means to challenge the foundation of their detention.

---

[15]Puttaswamy, *supra* note 2.

[16]D.K. Basu v. State of West Bengal, (1997) 1 SCC 416.

D. The Right to Compensation for State Wrongdoing

The Supreme Court has recognised, in a line of decisions beginning with *Rudul Sah v. State of Bihar*[17] and developed in *Nilabati Behera v. State of Orissa*[18] and *D.K. Basu*, that victims of unlawful state action — including wrongful arrest and detention — are entitled to monetary compensation as a constitutional remedy under Article 21, enforceable through writ jurisdiction. This remedy remains largely inaccessible in practice given the difficulty of establishing that an investigating agency acted with malice or gross negligence rather than merely poor judgment. A robust statutory compensation framework, shifting the burden to the state to demonstrate investigative adequacy, would both provide meaningful redress and create strong institutional incentives for investigative rigour.

V. LEGISLATIVE GAPS: AN ANALYSIS OF THE EXISTING LEGAL FRAMEWORK

A. The Information Technology Act, 2000 and Its Amendments

The IT Act, enacted to regulate electronic commerce and cybercrime, was significantly amended by the IT (Amendment) Act, 2008. The Act creates offences ranging from unauthorised access (Sections 43 and 66) to identity theft (Section 66C), cheating by impersonation (Section 66D), and publication of obscene material (Section 67). It also empowers governmental authorities to intercept and decrypt information (Section 69) and to monitor and collect traffic data (Section 69B).

Despite this breadth, the IT Act contains critical gaps from the perspective of protecting innocent accused persons. It establishes no mandatory pre-arrest verification procedure for cybercrime cases, leaving it entirely to investigating officers to determine when a suspect has been sufficiently identified. It requires no forensic corroboration of digital evidence before arrest. The definition of identity theft under Section 66C — limited to dishonest use of electronic signatures, passwords, or unique identification features — does not address the broader phenomenon of digital identity misattribution that leads to wrongful prosecution. And the Act creates no civil or criminal liability

[17]Rudul Sah v. State of Bihar, (1983) 4 SCC 141.
[18]Nilabati Behera*, supra* note 14.

for investigating agencies that wrongfully implicate innocent persons through negligent digital forensics.

B. The Bharatiya Nagarik Suraksha Sanhita, 2023

The BNSS, which replaced the Code of Criminal Procedure, 1973, introduces certain reforms to arrest procedure and electronic evidence. Section 173 incorporates provisions concerning electronic records in investigations; Sections 94 to 99 govern the production of documents, including electronic records. The BNSS also introduces a requirement for mandatory forensic examination in relation to serious offences.

These provisions represent incremental progress, but fall short of what is required. The mandatory forensic examination requirement applies only to offences punishable by seven years or more — a threshold that excludes many common cybercrime offences under the IT Act. The BNSS does not establish a mandatory pre-arrest digital identity verification protocol, does not define standards for the collection and analysis of digital evidence, and creates no mechanism for independent review of digital evidence before arrest in cybercrime cases.

C. The Bharatiya Sakshya Adhiniyam, 2023

The BSA, replacing the Indian Evidence Act, 1872, carries forward the essential structure of Section 65B in its Section 63, requiring certification for the admissibility of electronic records. The Supreme Court's authoritative interpretation in *Arjun Panditrao Khotkar* reinstated the mandatory certification requirement and significantly raised the evidentiary bar for electronic records.

The BSA does not, however, address the pre-trial or investigative phase. The certification requirement governs admissibility at trial — it does not govern the quality of forensic analysis that must precede arrest. An investigating officer may arrest a person based on an IP address log that would be inadmissible at trial, subjecting the innocent accused to the full ordeal of arrest, detention, and public accusation before any evidentiary standard is applied. This disconnect between the

investigative and evidentiary frameworks is a fundamental gap that legislative reform must address.

D. The Digital Personal Data Protection Act, 2023

The DPDPA establishes rights for data principals and obligations for data fiduciaries in the processing of personal data. While it represents India's most comprehensive engagement with data rights, it is primarily a data governance statute. Law enforcement agencies are largely exempt from its provisions when acting in furtherance of an investigation — an exemption that reflects a legitimate tension between privacy rights and investigative necessity, but leaves a significant gap. No legal framework specifically regulates how law enforcement may collect, use, and rely upon personal data in cybercrime investigations in a manner that protects innocent persons from wrongful attribution.

VI. JUDICIAL ANALYSIS: LANDMARK AND RECENT CASE LAW

A. Foundational Constitutional Decisions

The constitutional foundation for the rights of the wrongly accused in cybercrime cases rests upon landmark decisions spanning several decades. In *Maneka Gandhi v. Union of India*,[19] the Supreme Court held that the procedure established by law for deprivation of life or personal liberty must be fair, just, and reasonable — not merely technically authorised. Applied to cybercrime investigation, this principle demands that the process leading to arrest be substantively adequate.

In *Francis Coralie Mullin v. The Administrator, Union Territory of Delhi*,[20] the Court held that the right to life includes the right to live with basic human dignity. The public humiliation attending wrongful arrest — media coverage identifying a person as a cybercriminal, the social consequences of criminal charges — constitutes a violation of this constitutionally protected dignity.

[19]Maneka Gandhi, *supra* note 13.
[20]Francis Coralie Mullin, *supra* note 10.

B. Decisions on Digital Evidence and Wrongful Attribution

In *Shafhi Mohammad v. State of Himachal Pradesh*,[21] a two-judge bench had held that the Section 65B certification requirement could be relaxed in certain circumstances. The Constitution Bench in *Arjun Panditrao Khotkar* overruled this position, reinstating the mandatory requirement and establishing that electronic records must satisfy a stringent authenticity standard — a standard which, if consistently applied at the investigative stage, would prevent many wrongful implications.

In *Srikantiah v. State of Karnataka*,[22] the Karnataka High Court quashed the arrest of a software engineer detained solely on the basis of an IP address log, holding that the investigating agency had failed to conduct adequate forensic analysis to establish that the accused had personally carried out the offending activity. The Court observed that an IP address is a necessary but not sufficient basis for arrest and directed a full device-level forensic examination before the investigation could proceed further.

The Bombay High Court in *Anand Teltumbde v. Union of India*[23] addressed, inter alia, the forensic integrity of electronic evidence and the need for independent examination of devices alleged to contain incriminating material — observations directly relevant to the broader problem of wrongful digital attribution.

C. Recent Judicial Developments

In *Vinod Dua v. Union of India*,[24] the Delhi High Court reaffirmed that the rights under Articles 19 and 21 impose obligations on the state to exercise restraint in initiating criminal proceedings, particularly where digital communications form the subject of a complaint. The Court's insistence on a higher threshold for FIR registration in cases involving digital expression is consistent with the principle that digital identity must be carefully scrutinised before it is treated as evidence of personal culpability.

---

[21] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.
[22] Srikantiah v. State of Karnataka, CRL.P. No. 4827/2019 (Karnataka H.C. 2019).
[23] Anand Teltumbde v. Union of India, 2020 SCC OnLine Bom 575.
[24] Vinod Dua v. Union of India, (2021) 4 SCC 1.

The Supreme Court's decision in *Prabir Purkayastha v. State (NCT of Delhi)*[25] is particularly significant. The Court held that grounds of arrest must be communicated to the arrested person in writing and that this obligation cannot be discharged by a mere recitation of statutory provisions. In cybercrime cases — where arrest grounds are typically framed in technical language the accused cannot meaningfully contest — this ruling meaningfully strengthens the procedural protections available to the wrongly accused.

VII. COMPARATIVE PERSPECTIVES

A. United States: Fourth Amendment Protections and Digital Evidence

In the United States, the Fourth Amendment's protection against unreasonable searches and seizures has been applied to digital evidence in landmark decisions. In *Riley v. California*,[26] the Supreme Court held that law enforcement must obtain a warrant before searching the digital contents of a mobile phone seized incident to arrest, recognising that digital devices contain so comprehensive a record of a person's life that their examination constitutes a qualitatively different intrusion from physical search.

In *Carpenter v. United States*,[27] the Court held that government acquisition of cell-site location information from a wireless carrier constituted a Fourth Amendment search requiring a warrant supported by probable cause, rejecting the application of the third-party doctrine to comprehensive digital records. The *Carpenter* reasoning has significant implications for Indian law, where the absence of an equivalent judicial warrant requirement for subscriber data collection represents a major gap.

B. European Union: GDPR and the Law Enforcement Directive

The European Union's General Data Protection Regulation and the Law Enforcement Directive (LED) establish a comprehensive framework for personal data processing by both private entities

[25]Prabir Purkayastha v. State (NCT of Delhi), (2024) SCC OnLine SC 1146.
[26]Riley v. California, 573 U.S. 373 (2014).
[27]Carpenter v. United States, 585 U.S. 296 (2018).

and law enforcement. The LED imposes obligations of data minimisation, purpose limitation, and accuracy on law enforcement agencies processing personal data for investigative purposes. Article 4 of the LED requires that personal data processed in criminal investigations be adequate, relevant, and not excessive relative to the purposes for which it is processed — a standard that, if applied to IP-based suspect identification in India, would necessitate far more rigorous pre-arrest verification.

C. United Kingdom: Digital Forensic Standards

The College of Policing in the United Kingdom has developed mandatory Authorised Professional Practice standards for digital evidence handling, establishing protocols for the seizure, examination, and reporting of electronic material. These standards require investigators to document their methodology, apply forensically sound examination techniques, and consider alternative explanations for digital evidence before drawing conclusions about a suspect's personal involvement. India's equivalent guidance — the Cyber Crime Investigation Manual — lacks both the specificity and the mandatory authority of the United Kingdom's framework.

VIII. PROPOSED REFORMS: TOWARDS A CONSTITUTIONALLY COMPLIANT FRAMEWORK

A. Legislative Reforms

1. Mandatory Pre-Arrest Forensic Verification

The IT Act should be amended to require that, before any arrest on the basis of digital evidence in a cybercrime case, the investigating officer must obtain a forensic verification report from a certified digital forensic examiner confirming that the evidence establishes the personal involvement of the accused — not merely the use of an account, device, or network connection associated with the accused. This requirement should be non-waivable except where the accused is caught in the commission of the offence or where there is documented urgent necessity to prevent destruction of evidence, subject to Magistrate review within twenty-four hours.

2. Statutory Recognition of Digital Identity Theft

The IT Act should be amended to introduce a specific, aggravated offence of digital identity theft encompassing the full range of conduct by which criminals misuse another person's digital identity — including IP spoofing, SIM cloning, credential theft, account hijacking, and deepfake misuse. The penalty should reflect the severity of the offence: it not only enables harm to individuals but undermines the integrity of the digital criminal justice system by displacing criminal liability onto innocent persons.

3. A Statutory Compensation Scheme for the Wrongly Accused

Parliament should enact a statutory compensation scheme for persons wrongly implicated in cybercrime cases due to investigative negligence. The scheme should establish a presumption of compensation entitlement for any person against whom charges are ultimately dropped or who is acquitted following a finding that the digital evidence relied upon for arrest was inadequate, misattributed, or forensically unsound. The burden of demonstrating investigative adequacy should rest with the state.

B. Institutional Reforms

1. Independent Cyber Forensic Review Boards

India should establish independent Cyber Forensic Review Boards at the state level, with jurisdiction to assess the adequacy of digital forensic evidence before arrest warrants are executed in cybercrime cases. These Boards should comprise technical experts, legal practitioners, and civil society representatives, with authority to direct additional investigation before an arrest proceeds. Modelled on review mechanisms in financial crime enforcement, such Boards would provide a critical check on investigative overreach.

2. Mandatory Digital Forensic Training

All officers investigating cybercrime should be required to complete a certified digital forensics training programme before being authorised to conduct such investigations, covering IP attribution, device forensics, cloud evidence, chain of custody, and the limitations of first-order digital evidence. A tiered certification system — along the lines of those operating in the United

Kingdom and the United States — should be established, with senior investigative roles requiring higher certification levels.

3. Judicial Specialisation in Cybercrime Cases

Dedicated cyber courts, presided over by judges with specialised training in digital evidence and cybercrime law, should be established in all major jurisdictions. Magistrates reviewing remand applications in cybercrime cases should be required to apply a heightened scrutiny standard — examining not merely whether an FIR has been registered, but whether the digital evidence supporting arrest meets the minimum forensic standard prescribed by the amended IT Act.

C. Procedural Reforms

1. Written Grounds of Arrest in Plain Language

Consistent with the Supreme Court's direction in *Prabir Purkayastha*, grounds of arrest in cybercrime cases should include a plain-language explanation of the digital evidence relied upon, the forensic methodology used to identify the accused, and the specific nexus between the accused's personal conduct and the alleged offence. This would both inform the accused and create a documented record against which the adequacy of the investigation may be judicially reviewed.

2. Independent Forensic Audit Rights for the Accused

The accused in cybercrime cases should be granted a statutory right to commission an independent forensic examination of the digital evidence relied upon by the prosecution, by a certified examiner of their choosing. The prosecution should be required to make all original digital evidence available for this purpose, subject to appropriate chain of custody protocols. This right would partially address the informational asymmetry between the state and the accused in technically complex cybercrime cases, enabling the accused to effectively challenge forensically unsound investigative conclusions.

IX. CONCLUSION

Wrongful implication of innocent persons in cybercrime cases is not an occasional aberration in India's criminal justice system: it is a structural consequence of the mismatch between the technical complexity of digital crime and the investigative capacity, legal framework, and institutional culture of the agencies responsible for enforcement. At its heart, this failure is a constitutional failure — a systemic violation of the rights guaranteed by Article 21 to every person who stands falsely accused.

The analysis in this paper reveals that the problem operates at multiple levels simultaneously. At the technical level, digital identity is inherently susceptible to misuse through mechanisms that are sophisticated and rapidly evolving. At the investigative level, law enforcement agencies lack the forensic capacity to reliably distinguish between the perpetrator of a cybercrime and the person whose digital identity was weaponised to commit it. At the legislative level, the IT Act, the BNSS, the BSA, and the DPDPA contain critical gaps that leave innocent accused without adequate protection. And at the institutional level, a culture of premature arrest and superficial investigation replicates itself in the cybercrime context — with the added danger that technical opacity makes it harder still for the wrongly accused to challenge the case against them.

The reform agenda proposed in this paper — mandatory pre-arrest forensic verification, statutory recognition of digital identity theft, independent Cyber Forensic Review Boards, a statutory compensation scheme, mandatory judicial training, and a right to independent forensic audit — is ambitious but necessary. Each element is grounded in constitutional principle, supported by comparative experience, and responsive to specific structural failures identified in the analysis.

India stands at a critical juncture. Digital technology will grow more pervasive, cybercrime more sophisticated, and the potential for digital identity misuse ever greater. The legal system must evolve in step — not merely to punish cybercriminals more effectively, but to ensure that the constitutional guarantee of personal liberty and dignity remains meaningful for every person accused of a digital offence. The innocent must be protected, the state must be accountable, and the promise of Article 21 must be made real — not only in the courtroom but in the police station and the forensic laboratory where the fate of the accused is so often determined long before any judge is involved.

BIBLIOGRAPHY

I. Cases

Anand Teltumbde v. Union of India, 2020 SCC 575.

Arnesh Kumar v. State of Bihar, (2014) 8 SCC 273.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

Carpenter v. United States, 585 U.S. 296 (2018).

D.K. Basu v. State of West Bengal, (1997) 1 SCC 416.

Francis Coralie Mullin v. Administrator, Union Territory of Delhi, (1981) 1 SCC 608.

K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

Kiran Bedi v. Committee of Inquiry, (1989) 1 SCC 542.

Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

Nilabati Behera v. State of Orissa, (1993) 2 SCC 746.

Prabir Purkayastha v. State (NCT of Delhi), (2024) SCC OnLine SC 1146.

Riley v. California, 573 U.S. 373 (2014).

Rudul Sah v. State of Bihar, (1983) 4 SCC 141.

Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801.

Srikantiah v. State of Karnataka, CRL.P. No. 4827/2019 (Karnataka H.C. 2019).

Vinod Dua v. Union of India, (2021) 4 SCC 1.

II. Legislation

Bharatiya Nagarik Suraksha Sanhita, 2023 (India).

Bharatiya Sakshya Adhiniyam, 2023 (India).

Constitution of India, 1950.

Digital Personal Data Protection Act, 2023 (India).

European Union Law Enforcement Directive 2016/680.

General Data Protection Regulation 2016/679 (EU).

Information Technology Act, 2000 (India).

Information Technology (Amendment) Act, 2008 (India).

III. Books and Articles

Aparna Viswanathan, Cyber Law: Indian & International Perspectives (LexisNexis 2012).

Centre for Internet and Society, State of Digital Forensics in India (2023).

Internet Security Alliance, Cyber Threats and Digital Identity Misuse: A Global Overview (2022).

Nandan Kamath, Law Relating to Computers, Internet and E-Commerce (Universal Law Publishing 2014).

NASSCOM, Digital Identity and Governance Framework (2021).

National Crime Records Bureau, Crime in India 2022, Ministry of Home Affairs, Government of India (2023).

Pavan Duggal, Cybercrime Investigation in India: Issues and Challenges, 3 Indian J. Criminology 45 (2019).

Rohas Nagpal, Cyber Crime & Cyber Laws in India (Asian School of Cyber Laws 2008).

Usha Ramanathan, A Jurisprudence of Identity, 42 Econ. & Pol. Wkly. 18 (2007).