Page 698 - 714 **DOI:** *https://doi.org/10.63108/IJLMH.12907*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 5

2026

Identity Theft in the Digital Era and the Information Technology Act

DHARNA TEJASWINI[*] AND G. SRIKANTH[**]

ABSTRACT

Identity theft has emerged as a significant form of cyber-enabled wrongdoing as personal identity is increasingly represented through electronic credentials, passwords, account identifiers, mobile numbers, financial information and other digital attributes. The expansion of online banking, electronic commerce, social-media platforms, digital identity systems and cloud-based services has increased both the utility of personal information and the opportunities for its unlawful acquisition and misuse. Digital identity theft may facilitate impersonation, financial fraud, unauthorised access, account takeover and the commission of further offences. The legal problem consequently extends beyond the initial acquisition of information and encompasses attribution, electronic evidence, privacy, jurisdiction and victim remedies. This paper examines the Indian legal framework governing identity theft with particular emphasis on section 66C of the Information Technology Act, 2000 and its relationship with section 66D, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and the Digital Personal Data Protection Act, 2023. It analyses contemporary techniques including phishing, social engineering, social-media impersonation, financial identity theft, SIM-related compromise, data breaches and AI-assisted impersonation. The study adopts a doctrinal and analytical methodology and evaluates the interaction between substantive criminalisation, electronic evidence and constitutional rights. It argues that effective enforcement depends upon reliable attribution, preservation and authentication of digital evidence and a clear distinction between identity misuse, personation and related fraud. The paper proposes strengthened digital-forensic capacity, coordinated investigation, platform cooperation, victim-centred remedies and rights-sensitive regulation. It concludes that India's response to identity theft must combine technological adaptability with legality, privacy, proportionality and procedural fairness.

Keywords: *Identity Theft, Cybercrime, Information Technology Act 2000, Section 66C, Section 66D, Digital Identity, Electronic Evidence, Data Protection, Privacy, Artificial Intelligence*

[*] Author is a Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: https://orcid.org/0009-0009-3953-6690

[**] Author is a Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: https://orcid.org/0009-0000-2309-7018

 [ISSN 2581-5369]

I. INTRODUCTION

The rapid digitisation of everyday activity has transformed the nature of personal identity. Passwords, electronic signatures, authentication credentials, mobile numbers, banking identifiers and online accounts increasingly perform functions that were formerly performed by physical documents or face-to-face verification. When these identifiers are unlawfully obtained or used, the resulting harm may extend from financial loss to reputational injury, unauthorised access, privacy invasion and fraudulent transactions. Identity theft is consequently not merely a technical security problem; it is a legal problem involving autonomy, property, privacy and trust in digital institutions.[1]

The increasing dependence upon digital identifiers also changes the nature of vulnerability. A single compromised credential may provide access to several connected services, particularly where users reuse passwords or recovery mechanisms. The legal significance of identity theft consequently lies not only in the immediate loss suffered by a victim but also in the possibility that one compromised identifier can become an entry point into a wider sequence of unlawful conduct.[2]

Digital identity also has an institutional dimension. Banks, platforms, employers, government services and other entities rely upon authentication systems to determine whether a person is entitled to access an account or exercise a right. Identity theft undermines that trust relationship and may impose investigative and remedial costs on institutions as well as individuals.

The Information Technology Act, 2000 provides the principal specialised statutory response through section 66C, which addresses fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature. Section 66D separately addresses cheating by personation through a communication device or computer resource. These provisions frequently intersect with broader criminal conduct involving cheating, financial fraud, forgery and unauthorised access.[3]

The distinction between identity theft and related cyber offences is important for charging, investigation and adjudication. The same factual episode may contain several stages, but each stage must be examined according to the statutory ingredients applicable to it. Such an approach promotes precision and prevents the technological complexity of a case from obscuring the basic requirement of proving the offence alleged.[4]

---

[1] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[2] The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), § 66C.
[3] *Id.* §§ 66C, 66D.
[4] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

 [ISSN 2581-5369]

The contemporary legal environment has expanded through the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023 and the Digital Personal Data Protection Act, 2023. The first supplies the general substantive criminal-law framework; the second governs proof of electronic and digital records; and the third, once its substantive obligations are brought into force, will regulate the processing of digital personal data. Constitutional principles relating to privacy, dignity, equality, expression and fair procedure operate alongside these statutes.[5]

The evidentiary problem is intensified where the victim cannot explain how credentials were compromised. A prosecution may possess transaction records showing use of an account without possessing direct evidence of who obtained the credential. The resulting gap between system-level evidence and human attribution is one of the central issues examined in this paper.[6]

Existing scholarship has examined cybercrime, identity theft, privacy, data protection and electronic evidence as connected but often separate subjects. The specific problem addressed here is the legal chain connecting digital identity misuse to provable individual criminal responsibility. That chain requires attention to the protected identifier, provenance, authenticity, attribution, mens rea and the statutory ingredients of the offence charged.[7]

The paper proceeds as follows. Section 2 examines the literature, methodology and analytical framework. Section 3 analyses the statutory architecture governing identity theft. Section 4 examines the principal forms and emerging techniques of digital identity theft. Section 5 considers evidentiary and investigative challenges. Section 6 evaluates judicial approaches and cyber-law jurisprudence. Section 7 addresses constitutional rights. Section 8 offers a critical assessment and recommendations. Section 9 concludes by restating the principal findings.

II. Literature Review, Methodology and Analytical Framework

A. Conceptualising digital identity theft

Identity theft may be understood as the unauthorised acquisition or use of identifying information for an unlawful purpose. In digital environments, identity is not represented by a single object but by a collection of credentials and data capable of authenticating or representing

[5] The Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023); The Bharatiya Sakshya Adhiniyam, No. 47 of 2023, India Code (2023); The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[6] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.
[7] The Information Technology Act, *supra* note 2, §§ 43, 66, 66C, 66D.

 [ISSN 2581-5369]

an individual. This makes digital identity theft conceptually broader than simple document fraud and brings it into contact with privacy, data protection, cybercrime and financial regulation.[8]

The literature on cybercrime generally treats identity misuse as part of a wider ecosystem of privacy violations, online fraud and unauthorised access. A useful legal analysis must nevertheless identify the precise point at which a privacy or security incident becomes conduct attracting criminal responsibility. This requires attention to statutory definitions, mental elements, evidentiary rules and the relationship between specialised and general criminal provisions.[9]

B. Nature and evolution of identity theft

Traditional identity fraud commonly depended upon forged or stolen physical documents. Digital systems have changed the phenomenon by permitting credentials to be copied, transmitted and reused remotely. Phishing, credential stuffing, account takeover, SIM swapping and data breaches can now be combined with social engineering to create highly convincing impersonations. Artificial intelligence adds a further layer by enabling synthetic text, audio, images and video.

Digital identity theft has also evolved from isolated acts of impersonation into networked schemes. Credentials may be harvested by one participant, sold by another, used by a third and monetised through financial intermediaries. This division of activity creates attribution difficulties because the person possessing the stolen information may not be the person who ultimately uses it.[10]

C. Research methodology and scope

This study adopts a doctrinal and analytical methodology. It examines the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, the Digital Personal Data Protection Act, 2023, the Constitution and relevant Supreme Court jurisprudence.[11] The study is confined primarily to digital or electronically mediated identity theft in India and does not assume that every use of another person's name or image constitutes the statutory offence of identity theft.

The doctrinal method is appropriate because the principal questions concern interpretation of legislation and judicial treatment of electronic evidence. The analysis also has an institutional

[8] *Puttaswamy*, *supra* note 1 (informational privacy).
[9] The Information Technology Act, *supra* note 2, § 66C; The Digital Personal Data Protection Act, *supra* note 5.
[10] The Information Technology Act, *supra* note 2, §§ 66C, 66D.
[11] The Bharatiya Nyaya Sanhita, *supra* note 5; The Bharatiya Sakshya Adhiniyam, *supra* note 5; The Digital Personal Data Protection Act, *supra* note 5; INDIA CONST. arts. 14, 19, 21.

 [ISSN 2581-5369]

dimension because enforcement depends upon police capacity, forensic infrastructure, cooperation from private entities and mechanisms for obtaining data across borders.

D. Analytical framework

The analytical framework is designed to avoid a purely technology-driven approach. Digital forensic findings are treated as evidentiary components that must be connected to legal elements. The framework therefore moves from identification of the relevant digital attribute to attribution, mental element and proof beyond reasonable doubt.[12]

The analysis follows a sequential framework: identification of the protected credential or unique identifier; proof of its connection with the victim; authenticity and integrity of the electronic material; attribution of the relevant conduct to the accused; proof of fraudulent or dishonest use where required; and proof beyond reasonable doubt. This framework separates technical leads from evidence sufficient to establish criminal liability.[13]

III. Statutory framework governing identity theft

A. Section 66C of the Information Technology Act, 2000

Section 66C is the central statutory provision specifically addressing identity theft. It applies to fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature. The offence therefore contains both an objective element concerning the use of an identifying feature and a mental element concerning the character of that use.[14]

Section 66C is significant because it directly recognises the misuse of digital authentication features as criminal conduct. Its language, however, requires the prosecution to identify the feature involved and to demonstrate that the accused made the prohibited use. The provision therefore does not eliminate ordinary questions of proof; rather, it gives those questions a specialised statutory setting.[15]

The statutory reference to fraudulent or dishonest use makes the character of the conduct legally significant. Investigators must therefore gather evidence capable of showing why the use was unlawful and how the accused acted in relation to the victim's credential. Evidence of financial benefit, deceptive communications or deliberate concealment may be relevant depending upon the facts, but each inference must be assessed against the entire record.

---

[12] *Anvar P.V.*, *supra* note 6; *Arjun Panditrao Khotkar*, *supra* note 6.
[13] *Sharad Birdhichand Sarda v. State of Maharashtra*, (1984) 4 SCC 116; *Kali Ram v. State of Himachal Pradesh*, (1973) 2 SCC 808.
[14] The Information Technology Act, *supra* note 2, § 66C (penalising fraudulent or dishonest use of the electronic signature, password or any other unique identification feature of any other person).
[15] *Id.*

 [ISSN 2581-5369]

The provision should not be reduced to mere possession of another person's information. The prosecution must establish the relevant identifying feature, its connection with another person, the accused's use of it and the fraudulent or dishonest character of that use. The practical difficulty often lies in attribution, especially where credentials have been compromised or devices are shared.[16]

B. Section 66D and cheating by personation

Section 66D addresses cheating by personation through a communication device or computer resource. Identity theft and personation can occur together but remain conceptually distinct. Section 66C focuses upon misuse of specified identifying credentials, whereas section 66D requires cheating by personation with the statutory technological nexus.[17]

Section 66D is particularly relevant where the offender communicates while representing himself or herself as another person. Personation can be persuasive even without sophisticated technical intrusion, because victims may respond to apparently authentic communications. The offence therefore occupies a different conceptual space from the unauthorised use of a password or other authentication feature.[18]

General criminal provisions remain relevant because identity theft may be a means to obtain property or induce another person to act. A legally coherent prosecution should identify the relationship between the cyber conduct and the resulting harm rather than treating the IT Act as an exhaustive code for every consequence of identity misuse.[19]

A digital incident may therefore support multiple offences where the facts establish separate statutory ingredients. The analysis should distinguish the acquisition of a credential, its later use, the false representation of identity and any resulting dishonest inducement.

C. Complementary provisions under the Bharatiya Nyaya Sanhita

The BNS provides general offences that may accompany digital identity theft, particularly cheating under section 318 and cheating by personation under section 319. Where digital impersonation results in delivery of property or forms part of a wider fraudulent scheme, the relevant BNS provisions may operate alongside the IT Act.

[16] *Shreya Singhal*, *supra* note 4.
[17] The Information Technology Act, *supra* note 2, §§ 66C, 66D.
[18] *Id.* § 66D.
[19] The Bharatiya Nyaya Sanhita, *supra* note 5, §§ 318–319 (cheating; cheating by personation).

 [ISSN 2581-5369]

D. Electronic evidence under the Bharatiya Sakshya Adhiniyam

Identity-theft cases depend heavily upon electronic records such as login histories, messages, emails, transaction records, platform data and device extractions. The BSA provides the current evidentiary framework for electronic and digital records. The legal question is not merely whether a record exists but whether its authenticity, integrity and connection with the disputed fact can be established.

Electronic evidence is indispensable because many identity-theft events leave their principal traces in information systems. Login timestamps, authentication events, transaction identifiers, email headers, device information and platform records can establish chronology and connections. Their evidentiary significance nevertheless depends upon lawful acquisition, reliability and a demonstrated connection with the disputed conduct.[20]

E. Data protection and the Digital Personal Data Protection Act

The DPDP Act addresses processing and protection of digital personal data within its statutory scope, although its substantive obligations are not yet in operation.[21] Its regulatory function differs from the criminal function of section 66C. A data breach may create conditions for identity theft, but the two legal events should not be treated as identical. The distinction is important for identifying whether the response should involve criminal prosecution, regulatory action, or both.

Data protection and criminal law address different regulatory problems. A security incident may create exposure to personal information even where no particular person has yet used it fraudulently. Conversely, an identity-theft offence may occur through a targeted compromise without a large-scale data breach. Keeping these categories distinct assists both regulators and investigators in selecting the appropriate response.[22]

IV. Digital identity theft and emerging techniques

A. Phishing, credential theft and social engineering

Phishing uses deceptive communications or websites to induce victims to disclose passwords, authentication codes or financial information. Social engineering supplements the technical

[20] The Bharatiya Sakshya Adhiniyam, *supra* note 5, §§ 61–63.

[21] The Digital Personal Data Protection Rules, 2025 (notified Nov. 13, 2025, published Nov. 14, 2025). By the commencement notification of the same date, §§ 18 to 26 and certain ancillary provisions commenced on publication; § 6(9) and § 27(1)(d) commence twelve months thereafter; and the remaining substantive provisions, including §§ 3 to 5, 6(1)–(8) and (10), and 7 to 17, commence eighteen months thereafter and are therefore not yet in operation.

[22] The Digital Personal Data Protection Act, *supra* note 5.

 [ISSN 2581-5369]

method by manipulating trust and urgency. The evidentiary inquiry should reconstruct the communication, identify the infrastructure used and connect the acquired credential with subsequent activity.

Phishing investigations should examine not only the final fraudulent transaction but also the communication pathway that produced the disclosure. Domain names, message headers, shortened links, hosting information, device records and subsequent authentication events can help reconstruct the sequence. Preservation is important because phishing infrastructure can disappear rapidly after an attack.[23]

B. Social-media impersonation and account takeover

Social-media identity theft may involve copying photographs and biographical information, creating deceptive profiles or taking control of an existing account. Not every false profile automatically falls within section 66C, because that provision specifically refers to an electronic signature, password or other unique identification feature. Depending upon the facts, personation, cheating or other offences may become relevant.[24]

Social-media impersonation illustrates the difficulty of applying a credential-focused provision to identity misuse that primarily concerns representation. Where an offender merely creates a misleading profile, the precise statutory basis must be identified from the conduct and resulting harm. Where an existing account is taken over through a stolen password, the analysis may be materially different.[25]

C. Financial identity theft and SIM-related compromise

Financial identity theft may involve unauthorised access to bank accounts, digital wallets, credit facilities or payment systems. SIM-related compromise can additionally interfere with one-time passwords and account-recovery mechanisms. Relevant evidence may include transaction records, authentication logs, device information, subscriber records and communications.

Financial identity theft frequently involves several institutions simultaneously. Banks may hold transaction information, telecommunications providers may hold subscriber information, platforms may hold communication records, and devices may contain authentication traces.

[23] The Information Technology Act, *supra* note 2, §§ 66C, 66D; *Anvar P.V.*, *supra* note 6.
[24] The Information Technology Act, *supra* note 2, §§ 66C, 66D; The Bharatiya Nyaya Sanhita, *supra* note 5, §§ 318–319.
[25] The Information Technology Act, *supra* note 2, § 66C (limited to the electronic signature, password or other unique identification feature of another person).

 [ISSN 2581-5369]

Effective investigation therefore depends upon timely coordination rather than reliance upon a single evidentiary source.[26]

D. Data breaches and synthetic identity

Large-scale data breaches may expose personal information that is subsequently combined with information from other sources. Synthetic identities may therefore be constructed from real and fabricated attributes. The legal challenge is to distinguish the initial compromise, subsequent possession, later misuse and the particular conduct attributable to an accused person.[27]

Synthetic identities create a further attribution problem because the identity used in a transaction may not correspond completely to any single real person. Investigators must establish which attributes belong to genuine individuals, how they were obtained and who assembled or used them. This makes provenance and chronology particularly important.[28]

E. Deepfakes and artificial intelligence-assisted impersonation

Generative AI has introduced realistic synthetic voices, images, video and messages. These technologies may increase the credibility of impersonation and complicate authentication. The appropriate evidentiary focus is provenance, source material, creation history, metadata, forensic indicators and corroborating evidence rather than visual or auditory realism alone.

AI-assisted impersonation creates a challenge for both investigators and courts because conventional visual or auditory inspection may be insufficient. Technical examination should be combined with source verification and independent corroboration. The legal question remains whether the relevant conduct satisfies the applicable offence, not simply whether a particular item of media is technologically sophisticated.

V. Evidentiary and Investigative Challenges

A. Authenticity and attribution of electronic evidence

The principal evidentiary problem is establishing that digital material is authentic and that the accused was responsible for the relevant activity. In *Anvar P.V. v. P.K. Basheer* and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court developed important principles concerning electronic evidence under the earlier statutory framework. The present BSA must be applied according to its own provisions while retaining the broader doctrinal concern with reliability and authentication.

---

[26] *Tehseen S. Poonawalla v. Union of India*, (2018) 9 SCC 501.
[27] *Puttaswamy*, *supra* note 1; The Digital Personal Data Protection Act, *supra* note 5.
[28] *Anvar P.V.*, *supra* note 6; *Arjun Panditrao Khotkar*, *supra* note 6.

 [ISSN 2581-5369]

The attribution problem is especially acute because digital systems record events rather than necessarily recording the human decision-maker behind each event. A login may demonstrate that credentials were used from a particular device or network, but further evidence may be required to identify who controlled that device at the relevant time. Courts should therefore examine digital evidence cumulatively rather than treating any isolated technical indicator as conclusive.[29]

B. Screenshots, metadata and digital records

Screenshots may establish what appeared on a screen but may not establish the original source, author, date or integrity of the underlying communication. Platform records, server logs, message identifiers, metadata and forensic images can provide stronger evidence when properly obtained and authenticated. Digital material should therefore be presented as part of a documented evidentiary chain.[30]

Digital records also have different evidentiary qualities. A screenshot is a representation made by a user, whereas a server log may be automatically generated by an information system. Neither category is automatically conclusive. The relevant inquiry concerns the circumstances of creation, preservation, reliability and connection with the fact in issue.[31]

C. Chain of custody and digital forensics

Where devices are seized, investigators should document seizure, storage, forensic imaging, extraction and transfer. Hash values and documented forensic methodology can assist in demonstrating integrity. Expert evidence should explain both the findings and their limitations.

Chain of custody is particularly important where the prosecution relies upon seized devices. Investigators should be able to explain when a device was obtained, how it was isolated from alteration, how a forensic image was created and how the extracted material was preserved. A transparent forensic process assists the court in evaluating both reliability and the possibility of contamination.[32]

D. *Mens rea* and individual attribution

Identity-theft prosecution requires attention to the mental element prescribed by the offence. Repeated access, concealment, financial benefit, deceptive communications and coordinated conduct may support an inference of fraudulent or dishonest purpose, but the inference must

[29] *Anvar P.V.*, *supra* note 6; *Arjun Panditrao Khotkar*, *supra* note 6.
[30] *Anvar P.V.*, *supra* note 6.
[31] *Arjun Panditrao Khotkar*, *supra* note 6.
[32] The Bharatiya Sakshya Adhiniyam, *supra* note 5, §§ 61–63.

 [ISSN 2581-5369]

arise from the complete evidentiary record. A device, account or IP address should not automatically be equated with the human actor.

The mental element cannot safely be inferred merely from possession of another person's data. Evidence of repeated use, concealment, financial gain or coordination may strengthen an inference of dishonest purpose, but the inference must remain grounded in proven circumstances. This is consistent with individualised criminal responsibility and the presumption of innocence.[33]

E. Jurisdiction and cross-border investigation

Digital identity theft can involve a victim in one jurisdiction, an offender in another, a platform in a third jurisdiction and financial intermediaries elsewhere. Section 75 of the IT Act provides an extraterritorial basis in specified circumstances,[34] but legal reach does not eliminate the practical problems of obtaining overseas records, identifying foreign offenders or securing cooperation.

Cross-border identity theft demonstrates the difference between legal jurisdiction and practical investigative capacity. Even where Indian law applies, relevant evidence may be held by foreign entities or located on infrastructure outside India. Delays in obtaining such material may affect both the prosecution and the accused's ability to test the evidence, making procedural cooperation important.

VI. JUDICIAL APPROACH AND EMERGING CYBER-LAW JURISPRUDENCE

A. Electronic evidence and judicial proof

Indian jurisprudence establishes that electronic material is not self-proving merely because it is technologically generated. Courts must consider statutory requirements, authenticity, integrity, relevance and the connection between the record and the fact to be proved. This is particularly important in identity-theft cases where digital records may constitute the principal evidence of attribution.

Judicial treatment of electronic evidence reflects the principle that technological form does not itself establish evidentiary reliability. The court must examine the governing statutory requirements and the relationship between the electronic record and the fact to be proved. This is particularly important when the record is the principal basis for attributing conduct to an accused.[35]

---

[33] The Information Technology Act, *supra* note 2, § 66C; *Kali Ram*, *supra* note 13.
[34] The Information Technology Act, *supra* note 2, § 75.
[35] *Anvar P.V.*, *supra* note 6; *Arjun Panditrao Khotkar*, *supra* note 6.

 [ISSN 2581-5369]

B. *Anvar P.V.* and *Arjun Panditrao Khotkar*

Anvar P.V. and *Arjun Panditrao Khotkar* are important authorities for understanding the evidentiary treatment of electronic records under the former Evidence Act. Their continuing significance lies in the insistence that electronic evidence must satisfy the applicable statutory framework and that courts should not treat electronic copies as automatically reliable.

The importance of *Anvar P.V.* and *Arjun Panditrao Khotkar* lies in the Supreme Court's sustained attention to the statutory treatment of electronic records. Although the current evidentiary regime is the BSA, the jurisprudential emphasis on authenticity, statutory compliance and reliability remains useful when analysing digital material.[36]

C. Privacy and informational autonomy

Justice K.S. Puttaswamy (Retd.) v. Union of India[37] recognised privacy as a constitutionally protected interest. Identity-theft investigations can expose communications, financial information, photographs, contacts and other personal records. Law-enforcement access to such information must therefore remain subject to applicable legal safeguards and constitutional limitations.

Privacy considerations arise at multiple stages of an identity-theft investigation. Investigators may seek access to a suspect's devices, financial information and communications, while records of other individuals may be incidentally collected. Constitutional safeguards therefore require attention to the scope and purpose of investigative access.

D. Online expression and digital impersonation

Shreya Singhal v. Union of India[38] demonstrates the importance of precision when the State regulates online expression. Identity-related conduct may overlap with pseudonyms, parody or criticism. The legal framework should distinguish deceptive impersonation intended to produce unlawful consequences from protected forms of communication.

Digital impersonation must also be distinguished from lawful online expression. A pseudonym or parody may resemble impersonation at a superficial level without containing the dishonest inducement or credential misuse required by a criminal provision. Legal analysis should therefore focus on the conduct and statutory ingredients rather than the mere appearance of another person's identity.

---

[36] *Anvar P.V.*, *supra* note 6; *Arjun Panditrao Khotkar*, *supra* note 6.
[37] *Puttaswamy*, *supra* note 1.
[38] *Shreya Singhal*, *supra* note 4.

 [ISSN 2581-5369]

E. Individualised criminal responsibility

Judicial assessment should remain focused on the particular accused. Association with a compromised account, possession of a device or connection with a telephone number may be relevant but does not, without corroboration, necessarily establish authorship or fraudulent use. The court must evaluate the complete evidentiary chain.

Individualised attribution is essential because shared devices, compromised accounts and network-level identifiers can create false associations. The judicial task is to determine whether the evidence, considered as a whole, connects the accused to the relevant act and mental element. This protects the accuracy of adjudication while allowing reliable digital evidence to perform its proper role.[39]

VII. CONSTITUTIONAL RIGHTS AND RIGHTS-SENSITIVE REGULATION

A. Articles 14, 19 and 21

Articles 14, 19 and 21 provide an important constitutional framework for identity-theft enforcement. Article 21 protects life and personal liberty and encompasses privacy; Article 14 requires non-arbitrary state action; and Article 19 protects expression subject to constitutionally permitted restrictions.[40]

Article 14 is relevant because enforcement practices must not become arbitrary or inconsistent. Article 19 becomes relevant where regulation or investigative action affects protected forms of communication, while Article 21 provides the principal constitutional setting for privacy and personal liberty. These provisions operate together with statutory safeguards rather than existing as abstract principles separate from cybercrime enforcement.

B. Privacy, dignity and informational autonomy

Digital identity is intertwined with communications, financial information, photographs and behavioural data. Protection against identity theft therefore protects more than economic interests; it protects the individual's ability to maintain control over information associated with the self. At the same time, investigative access must remain lawful and proportionate.

Informational autonomy has particular importance because digital identity consists of information about a person's relationships, finances, communications and activities. Unlawful appropriation may therefore interfere with personal autonomy even when the immediate

[39] *Sharad Birdhichand Sarda*, *supra* note 13; *Kali Ram*, *supra* note 13.
[40] INDIA CONST. arts. 14, 19(1)(a), 21; *Puttaswamy*, *supra* note 1.

 [ISSN 2581-5369]

financial loss is modest. Effective legal protection should consequently recognise both economic and dignitary dimensions of identity theft.[41]

C. Fair trial and presumption of innocence

Technological evidence can create an appearance of precision even where alternative explanations remain possible. A device, IP address, account or transaction may provide an investigative connection without conclusively proving authorship. The accused must retain a meaningful opportunity to challenge authenticity, attribution and interpretation.

Fair trial principles require the accused to be able to contest the prosecution's digital evidence. Technical terminology should not obscure the need to explain how the evidence was generated, collected and interpreted. Where reasonable alternative explanations exist, the court must evaluate them according to the applicable criminal standard rather than assuming that technological evidence is infallible.[42]

D. Balancing cybersecurity and fundamental rights

Effective cybercrime enforcement must protect individuals without permitting indiscriminate collection or retention of unrelated personal information. A rights-sensitive model requires lawful authority, legitimate purpose, necessity, proportionality and accountability in the use of investigative technologies.

A balanced regulatory framework should distinguish necessary investigation from indiscriminate data collection. Necessity, proportionality, lawful authority and accountability provide safeguards against excessive intrusion while permitting legitimate cybercrime investigation. Such safeguards can also improve public confidence in digital enforcement institutions.[43]

VIII. Critical assessment and recommendations

A. Principal findings

India has a specific offence of identity theft under section 66C and a related technological personation offence under section 66D.[44] The wider statutory framework can address associated cheating, forgery, unauthorised access and data-related conduct. The principal practical difficulty is transforming rapidly changing digital activity into reliable proof of individual culpability.

---

[41] *Puttaswamy*, *supra* note 1.
[42] *Kali Ram*, *supra* note 13; *Sharad Birdhichand Sarda*, *supra* note 13.
[43] *Puttaswamy*, *supra* note 1; *Shreya Singhal*, *supra* note 4.
[44] The Information Technology Act, *supra* note 2, §§ 66C, 66D; The Bharatiya Nyaya Sanhita, *supra* note 5.

 [ISSN 2581-5369]

The principal statutory framework is capable of addressing many conventional forms of identity misuse, but technological change creates new factual patterns that may not fit neatly within existing categories. The response should therefore focus not only on creating additional offences but also on improving interpretation, evidence collection and institutional coordination.

B. Digital forensic and investigative capacity

Investigating agencies should strengthen forensic laboratories, standardise evidence-preservation procedures and improve capacity in mobile forensics, cloud evidence, financial tracing and account attribution. First-response officers should be trained to preserve volatile evidence and document the circumstances of seizure and extraction.

Forensic capacity should extend beyond basic device examination. Investigators increasingly require skills relating to cloud services, mobile applications, account recovery systems, cryptocurrency or digital-payment trails where relevant, and platform-generated records. Training should be continuous because investigative methods can become obsolete as rapidly as the technology itself.[45]

C. Platform, financial and telecommunications cooperation

Identity theft often crosses institutional boundaries. Timely cooperation among law-enforcement agencies, banks, payment intermediaries, telecommunications providers and digital platforms can assist in preserving records, securing compromised accounts and tracing fraudulent transactions. Such cooperation should operate through clear legal processes and appropriate privacy safeguards.

Cooperation with platforms and financial institutions is particularly important during the early stages of an incident. Prompt preservation of logs and transaction information can materially affect the availability of evidence. Cooperation should, however, remain subject to clear legal authority and safeguards concerning the disclosure of unrelated personal information.

D. Victim-centred remedies

Victims require accessible reporting mechanisms, rapid account-security measures and assistance in addressing continuing financial or reputational harm. Early preservation of digital evidence should be integrated with victim assistance because delay may result in deletion of records or further misuse of the identity.

Victim-centred remedies should address the continuing nature of identity misuse. An account may remain compromised after the first fraudulent transaction, and a false profile may continue

[45] *Anvar P.V.*, *supra* note 6; *Arjun Panditrao Khotkar*, *supra* note 6.

 [ISSN 2581-5369]

to cause reputational harm after a complaint is registered. Reporting systems should therefore connect investigation with practical steps for securing accounts and preserving evidence.

E. Legislative and institutional reform

Future reform should clarify the interaction between section 66C, section 66D, general criminal offences, electronic-evidence rules and data-protection obligations. Clear guidance on AI-assisted impersonation, synthetic identities and cross-border evidence would reduce uncertainty while preserving the principle of legality.

Legislative reform should be guided by the principle of legality. New forms of technology should not automatically produce new criminal liability unless the statutory ingredients are satisfied. At the same time, where recurring forms of harmful conduct expose a genuine legislative gap, Parliament may consider precise amendments supported by clear definitions and safeguards.

F. Proposed rights-sensitive evidentiary model

A coherent model should proceed sequentially: identify the protected credential; establish its connection with the victim; preserve and authenticate the relevant digital record; attribute the conduct through multiple corroborating sources; establish the required mental element; identify the applicable offence; and evaluate the evidence against the criminal standard of proof. This model helps prevent technical association from being converted into automatic criminal liability.

The proposed evidentiary model provides a practical bridge between technology and criminal law. It encourages investigators to establish the identity of the protected credential, preserve the source material, corroborate attribution and identify the mental element before drawing legal conclusions. This sequence can improve both prosecution quality and protection against mistaken attribution.

IX. Conclusion

Identity theft lies at the convergence of personal identity, technology and criminal law. The Information Technology Act, 2000 remains central through sections 66C and 66D, while the Bharatiya Nyaya Sanhita, the Bharatiya Sakshya Adhiniyam and the Digital Personal Data Protection Act address complementary aspects of criminal liability, electronic evidence and data governance.

The legal significance of identity theft lies in the interaction between individual identity and the systems of digital authentication. The stakes of a compromise rise as more critical activities

 [ISSN 2581-5369]

come to depend upon digital credentials. The law must respond to these risks without assuming that every digital identity incident is the same, or that a single statutory provision can cover every stage in a complex scheme.

Reliable attribution must remain at the heart of the matter. Digital evidence can be powerful, but its value depends upon provenance, integrity, context and connection with the accused. The prosecution must be able to rely upon admissible and adequately corroborated evidence to prove the offence, and not merely upon its technological appearance.

A password, account, device, IP address or transaction may be an important link in an evidentiary chain, but none should be treated as conclusive proof of authorship. Authenticity, integrity, attribution and the applicable mental state must be proved according to law.

The future framework should combine clarity of substance, effectiveness of investigation and constitutional restraint. Robust forensic institutions and coordinated reporting can enhance enforcement, while privacy, fair trial, freedom of expression and the presumption of innocence safeguard the legitimacy of the response. The goal is therefore a system that can adapt to technological change while continuing to apply stable principles of legality and proof.

India's future response should combine effective digital investigation with constitutional safeguards. Better enforcement can be achieved through robust forensic practice, early preservation, institutional cooperation and victim-oriented remedies. Privacy, freedom of expression, fair trial and the presumption of innocence remain essential to legitimate cybercrime adjudication.

*****

 [ISSN 2581-5369]