



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer ~ Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

BEYOND CONSENT: ACCOUNTABILITY, THE 'GOLDEN HOUR,' AND THE NEW FRONTIER OF DATA PROTECTION

AUTHORED BY - ASWATHI.V.S

Guest Faculty at School of Law Pondicherry University,

CO-AUTHOR - NIHALA JASMIN K K

Practising Advocate

ABSTRACT

The Digital Personal Data Protection (DPDP) Rules, 2025 and the Information Technology (Intermediary Guidelines) Amendment Rules, 2025 herald a new chapter in India's digital social contract. This paper examines the growing problem of online theft of money and argues that our existing legal frameworks are becoming increasingly inadequate in response to a new form of invisible crime. This research critically examines the tripartite relationship between the citizen, bank and platform. Particularly, how the loss is not only unjustly borne by the citizen but also by the bank and platform as well.

Initially, we critique the notice-and-consent model, which has been a useful shield for the powerful for long. The Puttaswamy court judgment that enshrines privacy as an intrinsic facet of one's identity and dignity under Article 21 provides the crux of the argument. This dignity is violated when "consent" is manufactured through Dark Patterns or hijacked through vishing powered by AI. Amidst the new standard of real-time deepfake impersonation, the age-old 'reasonable man' standard in law is under siege if the human mind can no longer tell the difference between a son's voice and that of a machine clone 'consent' is vitiated initially in law.

The research also challenges the "Safe Harbor" safeguards normally enjoyed by social media intermediaries. The 2025 Amendments have, in our view, created a situation whereby platforms are expected to act as "proactive gatekeepers" owing to rules such as Rule 3(3) to label synthetic content in metadata. This paper shows the emerging judicial consensus that in cases of fraud a shift in onus should take place from the victim to the Data Fiduciaries who have the technical capability to prevent such frauds by analyzing the landmark judicial decision in Hare Ram Singh v. RBI (2024).

The research develops a "Proportionality-based Liability Framework" by combining the criminal deterrents from the Bharatiya Nyaya Sanhita 2023 with the DPDP Rules which set their regulatory requirements. It also tend to establish that State operations become responsible for damages when emergency systems break down during the essential "Golden Hour period" while platforms should be held Strictly Liable for their failures to maintain algorithmic safety. This study provides a plan for a digital world where individuals are more accountable and information privacy is a reality rather than merely a regulation.

Key words: Data Protection, privacy, fraud, safe harbour, Golden hour period.

INTRODUCTION

The digital economy has experienced rapid development which has caused people to define their identity through digital data and biometric information and artificial markers instead of using their physical existence. The new system provides businesses with exceptional operational efficiency yet it has created a new crime category which law enforcement agencies cannot address because traditional legal methods no longer apply. The paper argues that AI-driven financial fraud has reached epidemic proportions because the digital social contract between different groups failed to execute its monitoring responsibilities¹. The Indian legal system used Article 21 to protect physical freedom until the Puttaswamy decision brought a new requirement to interpret "Informational Self-Determination" as a fundamental element which supports human dignity².

The research evaluates Digital Personal Data Protection Rules 2025 and IT Intermediary Amendment Rules 2026 to demonstrate how the "notice-and-consent" system operates as a tool which companies use to create user consent through Dark Patterns³. The central argument posits that in the face of machine-speed deception like AI-vishing, the "Reasonable Man" standard is a legal fiction⁴. The study introduces a liability system which depends on proportionality to determine responsibility for losses. The framework establishes a three-part system which holds Banks accountable as fiduciaries and Platforms accountable as strict-liability gatekeepers and the State accountable as an administrative guarantor who protects victims during the "Golden Hour" period⁵.

¹ Digital Personal Data Protection Act, 2023.

² Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1(India).

³ Supra note 1.

⁴ Hare Ram Singh v. Reserve Bank of India, 2024 Supreme (Del) 865 (India).

⁵ Reserve Bank of India, Master Direction on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions, RBI/2017-18/15 (Issued on July 6, 2017).

1. The Constitutional Bedrock Informational Privacy as a Fundamental Right

1.1. The Evolution of Jurisprudence: From Freedom of Movement to Digital Identity

In the past, the Indian courts looked at Article 21⁶ in a narrow, physical way. During the A.K. Gopalan⁷ era in the 1950s, "personal liberty" meant little more than not being in physical chains. But as our lives moved into the digital economy, the law had to change what it meant by "body." Our digital selves—our data, our voices, and our footprints—became just as real as our physical selves.

The change really started with *Maneka Gandhi (1978)*⁸, when the Supreme Court said that any state interference with freedom had to be "just, fair, and reasonable." That order is our main protection in the world today. It makes sure that a person's digital trail, which includes things like voice patterns and biometrics, is more than just technical data. These aren't just bits of information; they are important parts of who we are and what we stand for⁹.

1.2. The Post-Puttaswamy Model and the Right to Information Self-Determination

The landmark nine-judge bench ruling in *Justice K.S. Puttaswamy v. Union of India*¹⁰ marked the turning point for a digital right to privacy. The Court went beyond the passive "right to be let alone" and came up with the strong idea of Informational self-determination. This principle says that people have a natural right to decide who can see and use their personal information. The Court ruled that privacy is an inherent aspect of human dignity. This means that when someone's data is used for something like making a deepfake, it is not only a financial loss but also a direct attack on that person's dignity and their right to keep their real public and private identity.

1.3. The Proportionality Test protects the rules.

The Puttaswamy judgment¹¹ did more than just say that people had a right; it also set up a strict three-part test to see if any state-mandated invasion of privacy, like e-KYC or mandatory metadata tracking, was okay. First, the measure must be legal, which means that there must be

⁶ India Const. art. 21.

⁷ A.K. Gopalan v. State of Madras , AIR 1950 SC 27 (India).

⁸ Maneka Gandhi v. Union of India ,(1978) 1 SCC 248 (India).

⁹ Supra note 2.

¹⁰ *Id.*

¹¹ Supra note 2,para .325.

a clear set of laws that support it, like the Digital Personal Data Protection (DPDP) Act of 2023. Second, it needs to have a good reason, like keeping the country safe or stopping financial fraud. The third requirement is proportionality, which means that the state must use the "least restrictive" means to reach its goal. This framework is needed to look at AI-based fraud-tracking systems and make sure that the search for safety doesn't turn into an unconstitutional state of total surveillance¹².

1.4 When AI Hijacks Our Brains: The Death of Real Choice

In the world we live in now, the most important part of our rights under Article 21¹³ is the simple freedom to make our own choices without someone else pulling the strings. But AI-vishing and deepfakes have completely broken that. We aren't just talking about a simple scam here; we're talking about a "fake reality" that's designed to mess with our heads.

The law specifically the Indian Contract Act says that "consent" is only real if you give it freely¹⁴. If you aren't being lied to or tricked, you're in control¹⁵. But when you hear a family member's voice created by a machine begging for money, you aren't actually "choosing" to send that cash. Your brain is being hijacked. You're reacting to a manufactured nightmare, not making a logical decision.

The Delhi High Court finally called this out in the *Hare Ram Singh v. RBI*¹⁶ case last year. They basically told the banks to stop blaming the victims for being "careless." The Court finally realized that when AI manipulates the way a human being thinks, it's not just a technical error it's a direct attack on our dignity and our right to be the masters of our own minds.

2. Statutory Framework, The DPDP Rules 2025 & IT Act Amendments

2.1 Institutionalizing Agency in the Digital Age

The Digital Personal Data Protection (DPDP) Rules 2025¹⁷ official notification marks the conclusion of the period during which digital contracts existed as non-negotiable agreements. Data Fiduciaries must now provide Standalone Notices under Rule 3 which must be shown separately from all other content including general terms and conditions¹⁸. The notices must be

¹² Manish Kumar, Digital Surveillance Vs. Privacy Rights: Constitutional Limits Post-Puttaswamy, 7 IJLLR 4982, 4983 (2025).

¹³ Supra note 6.

¹⁴ Indian Contract Act, 1872, s. 10.

¹⁵ *Id.* at s. 14.

¹⁶ *Hare Ram Singh vs. Reserve Bank Of India*, 2024 SCC OnLine Del 8039 (India).

¹⁷ Digital Personal Data Protection Rules, 2025.

¹⁸ *Id.* at Rule 3(1).

presented as separate items which must be translated into local languages and which must provide detailed information about the data being collected and its intended use¹⁹. The law establishes a total ban on "Bundled Consent" which forces users to accept complete privacy policies through a single click²⁰. Rule 3 mandates that organizations must obtain user consent through specific purposes which makes all consent obtained through "Dark Patterns" and complicated legal language invalid from the start²¹. The Consent Manager framework establishes a protection system which Rule 4 establishes as official protection²². The regulated entities function as fiduciaries for citizens by providing an interoperable platform which enables users to manage their consent across multiple services while maintaining control over their personal information.²³

2.2 From Passive Pipes to Proactive Gatekeepers: IT Amendment Rules 2026

The IT Rules will change in 2026, and platforms will no longer have the broad "Safe Harbor" protections that Section 79 used to give them²⁴. The law now puts all AI-generated content, from deepfake videos to vishing audio, under the strict category of Synthetically Generated Information (SGI)²⁵. This isn't just a label. It makes intermediaries "gatekeepers" who have to find and tag this content with permanent metadata²⁶. If a platform doesn't include a label or a provenance marker, they lose their immunity²⁷. This change is huge when it comes to AI-driven financial fraud. If a platform doesn't flag synthetic content that later helps a scam, it goes from being a neutral host to being careless²⁸. Not labelling is not only a mistake according to the 2026 rules; it is also a crime of negligence²⁹.

2.3. The 3 Hour "Golden Hour" Mandate and the Civil Trail

The "3-Hour Takedown Rule" is a big change to the rules for regulating SGI that came with

¹⁹ *Id.* at Rule 3(2).

²⁰ Digital Personal Data Protection Act, 2023, s. 6(1).

²¹ Digital Personal Data Protection Rules, 2025, Rule 3(3).

²² *Id.* at Rule 4.

²³ *Id.* at Rule 5.

²⁴ Information Technology Act, 2000, s.79.

²⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Rule 2(1)(wa).

²⁶ *Id.* at Rule 3(3).

²⁷ See *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

²⁸ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Rule 7.

²⁹ *Id.*

the 2026 Amendments³⁰. The legislature has created a technical "Golden Hour" that is necessary for effective victim restitution by shortening the previous 36-hour window to just three hours³¹. This law is important because it makes a legal connection to the Consumer Protection Act of 2019. If a fiduciary doesn't follow this faster timeline, it's now clear proof of a "deficiency in service"³². When read with Rule 7 of the DPDP Rules, 2025, which says that people must be told about a breach within 72 hours, it becomes clear who is responsible for the "civil trail."³³ Because of this synergy, the burden of proof is on the entity that is technically better. This means that platforms are fully responsible for any financial loss that a consumer suffers because they didn't follow the rules³⁴.

3. AI-Driven Vishing-The Vitiating of Consent

3.1 The Mechanics of AI-Vishing: Fake Identity and Deception Taking over.

AI-vishing uses neural networks to create voice clones of a person through their voice pitch and speech patterns which can be extracted from two audio samples³⁵. People who want to scam others prefer AI-vishing because it enables them to create deceptive digital avatars who imitate actual people that their targets trust³⁶. Regular scams use people and generic scripts. The clones create an experience that tricks brains into believing everything appears normal when they function in real time. This ability makes it possible to create highly convincing attacks which use personal trust as a technical method to deceive people. The fraudster obtains victim information while taking complete control of their relational identity which results in a change of their thought process because detection methods based on common knowledge and digital literacy training become ineffective³⁷.

3.2 The Doctrine of Vitiating Consent in Section 14

The main legal problem with AI-vishing is whether the victim's permission is valid³⁸. Section 13 of the Indian Contract Act of 1872 says that consent needs consensus ad idem, which means

³⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, Rule 3(1)(d).

³¹ *Id.*

³² Consumer Protection Act, 2019, s. 2(11).

³³ Digital Personal Data Protection Rules, 2025, Rule 7.

³⁴ Hare Ram Singh v. Reserve Bank of India, 2024 SCC OnLine Del 8039 (India).

³⁵ Supra note 25.

³⁶ Fatma Zehra & Eesha Kaul, Artificial Intelligence and the Law: Safeguarding Personality Rights in the Digital Age, 4 IJIRL, 984, 985 (2024).

³⁷ 896. SHAIKH ASHFAQ ET AL., DEFENDING AGAINST VISHING ATTACKS: A COMPREHENSIVE REVIEW FOR PREVENTION AND MITIGATION TECHNIQUES 411-422 (Pankaj Chandre et al. eds., 2024).

³⁸ Hare Ram Singh v. Reserve Bank of India, 2024 SCC OnLine Del 8039 (India).

that everyone agrees³⁹. But Section 14 says that consent must be "Free," and if it is gotten through "fraud" or "misrepresentation" it is not valid⁴⁰. In an AI-vishing situation, the victim's permission is based on a basic lie about who the other person is⁴¹. The AI clone is made to get around decisional autonomy, so the consent it gets is not legally valid, which means that any financial transaction that follows is voidable⁴².

3.3 Shifting the Burden: From Negligence to Institutional Fiduciary Duty

The transition from traditional caveat emptor to institutional liability shows a required development which technical knowledge gaps between citizens and sophisticated fraudsters compel⁴³. The ability of Generative AI to create synthetic fraud with high accuracy establishes the need for legal systems to differentiate between authentic agreements and fraudulent contract inducements⁴⁴. The RBI Zero Liability Principle defines "unauthorized electronic transfers" as including transactions which use high-fidelity voice cloning technology⁴⁵.

As per DPDP Act 2023 establishes a new relationship which identifies banks as "Data Fiduciaries" because they must maintain data protection at their highest responsibility⁴⁶. The Delhi High Court in *Hare Ram Singh v. RBI (2024)*⁴⁷ established this principle by denying defendants the rights to blame victims for "gross negligence" when they fell victim to advanced social engineering tactics. Justice Dharmesh Sharma demonstrated that AI-driven scams function beyond human understanding therefore security responsibilities must shift to institutional systems⁴⁸. Banks need to build synthetic fraud detection systems through their proactive algorithms which protect users' digital rights according to Article 21⁴⁹.

4. The Tripartite Liability Model

4.1. Financial Intermediaries: The Shift to Enhanced Fiduciary Duty

The modern banking system has moved beyond its traditional scope of being a simple custodian of money and has developed into the role of a Significant Data Fiduciary. As per the RBI

³⁹ Indian Contract Act, 1872, s.13.

⁴⁰ *Id.* at s.14.

⁴¹ *Id.* at s.17 (1).

⁴² *Id.* at s.19.

⁴³ *Hare Ram Singh v. Reserve Bank of India*, 2024 SCC OnLine Del 8039 (India)

⁴⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026.

⁴⁵ Reserve Bank of India, Master Direction - Consumer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (Issued on July 6, 2017) (India).

⁴⁶ Digital Personal Data Protection Act, 2023, s. 8 .

⁴⁷ *Hare Ram Singh*, 2024 SCC OnLine Del 8039, para. 34(India).

⁴⁸ *Id.*

⁴⁹ *Supra* note 6.

Master Directions, in conjunction with Section 8 of the DPDP Act, banks are under an elevated duty of care to protect the integrity of the financial ecosystem⁵⁰. The fiduciary duty in this instance arises in view of the failure of the system to identify and freeze "Mule Accounts," which are the lifeline of cyber-laundering. In the current AI-powered phishing attack, the "Reasonable Man" standard of prudent consumer behaviour is fast becoming obsolete; therefore, in the event that the bank's internal security mechanism fails to notify the bank of the unusual patterns of transactions that lie beyond the customer's historical data, the bank shall be held liable⁵¹.

According to the judicial dictum in the case of *Hare Ram Singh v. RBI (2024)*⁵², the onus of proof will shift, and the bank will be required to prove that it has shown "extraordinary diligence" to prevent the depletion of money, or else it will be held liable for a statutory claim of deficiency in service under the Consumer Protection Act, 2019⁵³.

4.2. Digital Platforms: The Doctrine of Strict Liability and Algorithmic Safety

The Information Technology (Intermediary Guidelines) Amendment Rules 2025 have developed into a system that eliminates all "Safe Harbor" protections which digital platforms used to access⁵⁴. The platforms under new Rule 3(3) track their activities as they function between two states which define their role as "proactive gatekeepers" and "passive conduits"⁵⁵. The strict liability should apply because platforms fail to identify SGI and they use deceptive "Dark Patterns" to steal financial assets⁵⁶. All user-interface designs which platforms use to create artificial user consent through their operational functions need to be established as invalid from the beginning because this design approach removes all protective powers which platforms hold under their intermediary status⁵⁷. The law establishes financial liability for organizations which create links between algorithmic safety and complete financial losses because untagged deepfake content and fraudulent advertisements which escape platform moderation lead to "financial siphoning" activities that end with actual damages⁵⁸. The shift in economic risk from innovation now protects users who face vulnerability while shifting

⁵⁰ Digital Personal Data Protection Act, 2023, s.8.

⁵¹ Manoj Roy Sarkar, The Evolving Landscape of Digital Privacy in India: Balancing Innovation and Data Protection by the Government, 9, *PusuIT*, 4 (2024).

⁵² *Supra* note 4, para .323.

⁵³ Consumer Protection Act, 2019, sec. 2(11), 2019.

⁵⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026

⁵⁵ *Id.* at Rule 3(3).

⁵⁶ Digital Personal Data Protection Rules, 2025, Rule 3(3).

⁵⁷ *Id.*

⁵⁸ *Supra* note 54, Rule 7.

accountability to those advanced technical systems which gain economic benefits from the ecosystem.

4.3. The State: Administrative Liability and the "Golden Hour" Mandate

The third element of the tripartite model is focused on the constitutional duty of the State to ensure that there is an effective remedy within the "Golden Hour," which is the first 120 minutes following the reporting of the crime when the recovery of the funds is still technically possible⁵⁹. The duty of the State is more administrative in nature and is dependent on the efficiency of the I4C/1930 Helpline (Indian Cyber Crime Coordination Centre) and the emergency response systems⁶⁰. If the citizen is punctual in reporting the crime, but the infrastructure of the State is inefficient because of technical delays, lack of coordination between the agencies, or system downtime, it amounts to a violation of the "Civil Trail" of accountability⁶¹. In the expanded interpretation of Article 21⁶², the failure of the State to have an operational emergency digital response system results in the permanent dissipation of the victim's assets which results in the inability to mitigate "identity theft" or freeze assets, the State will be held administratively liable for compensatory damages to ensure that the digital social contract is underpinned by a guarantee of administrative efficiency⁶³.

5. Judicial Trends and the Way Forward

5.1. Administrative Natural Justice

The judicial system has increased its involvement in protecting digital security because the legal framework now uses a "Proportionality-based Liability Framework" for assessment. The banking industry during 2025 saw its operations diligently executed through the implementation of audi alteram partem legal right. The 2023 decision *State Bank of India v. Rajesh Agarwal*⁶⁴ establishes a major legal precedent which has influenced high court rulings throughout 2025. The Supreme Court ruled that designating a bank account as "fraud" leads to "serious civil repercussions" which result in "civil death" for the account holder. The Court ruled that banks need to provide a show-cause notice before blacklisting or freezing accounts which requires them to issue a reasoned order.

⁵⁹ Supra note 2.

⁶⁰ Ministry of Home Affairs, Office Memorandum on I4C and Citizen Grievance Redressal, No. 22002/01/2021 (Issued on Jan 12, 2021).

⁶¹ Common Cause (A Regd. Society) v. Union of India, (1999) 6 SCC 667 (India).

⁶² Supra note 6.

⁶³ Nilabati Behera v. State of Orissa, (1993) 2 SCC 746 (India).

⁶⁴ State Bank of India v. Rajesh Agarwal, (2023) 6 SCC. 1 (India).

The judicial system needs a "Reasoned Order" because it prevents financial fiduciaries from using their authority without limits. The reasoned order requirement exists as a security measure which proves that the bank used its intellectual capacity to evaluate all information instead of relying on automated systems and vague police warnings. The courts expanded their interpretation of this principle to handle the complete account freezing situation which emerged during the 2025 period. Since it is "unjust and unwarranted display of power" the Delhi High Court ruled in *Malabar Gold and Diamond Ltd v. Union of India (2026)*⁶⁵ that freezing an entire account for a disputed amount is against the law. The current trend in the courts makes it clear that banks are "Significant Data Fiduciaries" whose job it is to stop fraud, but they are also administrative bodies that must follow the principles of natural justice.

5.2 The Post-Facto Safeguard

The research acknowledges the inherent tension between the "Golden Hour" requirement for immediate action and the deliberate pace of natural justice. Under the emerging "Way Forward" suggested by recent 2025-2026 rulings such as those by the Allahabad and Delhi High Courts posits a hybrid model of Proportionality, which says while a "debit freeze" may be initiated in the immediate wake of a cyber-report to prevent the dissipation of assets, it must be strictly limited to the disputed amount rather than the entire corpus of the account.

The emergency provisions of Section 106 of the BNSS⁶⁶ will lead to an account freeze which requires both the investigating agency and the bank to notify the jurisdictional magistrate within 24 hours while they must give the account holder a "Reasoned Notice" which started to enforce a strict "post-facto" transparency requirement by the courts. The "Civil Trail" of accountability maintains its strength because the system combines fast results with fair outcomes. The bank becomes a transparent intermediary that must prove its actions according to Articles 19 and 21 of the Constitution⁶⁷ which protect citizens' rights to trade and earn a living.

5.3 Beyond "Petty Theft" to Organized Fintech Crime

Digital fraud enforcement faces major difficulties because courts have traditionally treated digital fraud as single instances of "cheating" or "petty theft." Section 111 of the Bharatiya

⁶⁵ *Malabar Gold and Diamond Ltd. v. Union of India*, W.P.(C) 4198/2025 (Del. Jan. 16, 2026) (India).

⁶⁶ *Bharatiya Nagarik Suraksha Sanhita*, 2023, s.106.

⁶⁷ *Supra* note 6, art. 19(1) (g).

Nyaya Sanhita (BNS)⁶⁸ which launched in 2023 establishes "Organized Crime" as a criminal category. The statute now formally recognizes cyber-crimes and economic offenses like mass-marketing fraud and financial institution defraud schemes as organized criminal activities. The law recognizes current digital fraud operations as organized criminal networks which use advanced AI technology and international mule-account systems to defeat conventional security measures.

Section 111 of BNS establishes that any member of a syndicate who commits "continuing unlawful activity" will face extreme penalties which include life imprisonment and financial penalties that exceed basic restitution requirements. The law now considers digital fraud as organized crime because it operates through complete systems which endanger both state financial security and individual citizen rights.

5.4 The Necessity of a Unified Fintech Crime Code

In order for the "Proportionality-based Liability Framework" to be fully functional, India must have a "Unified Fintech Crime Code" since the current legal framework is still too fragmented among the IT Act, BNS, and DPDP Rules. This code would integrate the various definitions of digital fraud, platform negligence, and fiduciary duty into a single, harmonious legal document. The need for such a code is evident during the "Golden Hour" of a cyber-attack, the victim should not have to contend with a complex of jurisdictional overlaps between criminal law (BNS) and civil regulations (DPDP). The Unified Code would establish a seamless process for both the criminal prosecution of the perpetrator and the civil compensation of the aggrieved party. It would require that a "Deficiency in Service" on the part of a bank, as defined in the historic *Hare Ram Singh v. RBI (2024)*⁶⁹ case, automatically initiate a targeted recovery procedure. In this way, we can ensure that the "Civil Trail" of responsibility is as rapid and automated as the fraud itself.

Suggestions

- The Friction-by-Design requirement forces a 15-minute verification delay for voice command transactions and third-party link transactions to defend against AI-vishing threats which create immediate pressure.
- The IT Amendment Rules 2026 should be revised to create strict liability requirements

⁶⁸ Bharatiya Nyaya Sanhita, 2023,s. 111.

⁶⁹ Supra note 4.

for platforms whose algorithms increase fraudulent activities because these platforms will be treated as partners in criminal activities.

- The Digital Indemnity Fund creates a national fund which payment providers will fund to deliver immediate payments that protect the State's obligation as an administrative guarantor under Article 21.
- The Unified Fintech Crime Code should include a "Reverse Onus" provision that requires banks to prove their "AI-resilient" systems after synthetic fraud has been established against them.

Conclusion

The criminal world now experiences a new phase because advanced AI technology has become part of its operations, which transforms cyber-fraud from its former status as "petty theft" to a new serious danger that endangers the financial stability of the Republic. The research findings in this paper demonstrate that the crisis solution requires a complete system of responsibility which needs to be implemented through unified rules instead of existing disconnected laws. The two court cases of *Hare Ram Singh v. RBI (2024)* and *SBI v. Rajesh Agarwal* demonstrate that courts now agree that whenever people lack technological knowledge their technical abilities should determine legal responsibilities. The 2026 IT Amendments introduce "Proactive Gatekeeping" which replaces "Safe Harbor" protections to establish new standards for intermediary liability in digital business operations that generate profits.

The way forward lies in the formalization of a Unified Fintech Crime Code and the rigorous enforcement of the 3-Hour "Golden Hour" Mandate. India can establish a "Civil Trail" of accountability that operates with fraud detection speed through the combination of Section 111 criminal deterrents from the BNS 2023 with DPDP Rules administrative requirements. The digital age requires regulatory frameworks which will safeguard digital property rights of citizens as this protection represents an essential constitutional right. The law needs to protect privacy and property as essential human rights if we want to maintain Article 21 protection.