JOURNAL OF CYBER GOVERNANCE AND INTELLECTUAL PROPERTY

Volume 1, Issue 2 **Article 8**

Cyber Governance and Digital Financial Fraud Against Senior Citizens: Assessing India's Regulatory and Institutional Framework

Vaibhav Sharma

Greater Noida Academy of Legal Studies and Research, Greater Noida

Recommended Citation:

Sharma (2026) "Cyber Governance and Digital Financial Fraud Against Senior Citizens: Assessing India's Regulatory and Institutional Framework" Journal of Cyber Governance and Intellectual Property, Vol. 1, Issue 2, Article 8. (DOI)

ABSTRACT

This article focuses on technology-enabled financial fraud in India and examines how criminals commit and organise these crimes. The article examines the provisions of the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 (DPDP Act), and Maintenance and Welfare of Parents and Senior Citizens Act, 2007. The key findings focus on Financial scams like phishing and need for digital protection from crimes like Digital arrest. This article will provide insights into the efforts taken by international laws and agreements related to jurisdiction and will provide information on how Budapest convention and California consumer privacy act and GDPR that is of EU. These laws provide individuals with greater control over their personal data.

KEYWORDS

Information Technology Act, 2000; Digital Personal Data Protection Act, 2023 (DPDP Act); Phishing; Digital arrest; Financial scams; Maintenance and welfare of parents and senior citizens act, 2007

INTRODUCTION

Today, many crimes are committed through digital means. India ranks second globally, in terms of cybercrime and phishing attacks, according to reports by Meta's Adversarial Threat Report and Zscaler ThreatLabZ.[1] Financial fraud against elderly persons has increased with the rapid adoption of modern technology, including UPI and digital banking Recent forms of technology-enabled fraud include digital arrest scams and OTP scams. The increased affordability and accessibility of the internet following the entry of Reliance Jio into the Indian market on 5 September 2016 made people more reliant on technology. This increased reliance on technology also contributed to the rapid growth of cybercrime with this the cyber-crimes also rose rapidly. It grew large by the affordable internet that was provided and by JIO in 2016 which was free for almost until March 31 2017 under a happy new year offer.[2] In India there is a lack of awareness regarding the cyberlaws and the cyber-crimes that happen in India. According to a PwC's Indian survey on data privacy only 16% of the people know about the Digital Personal Data Protection Act, 2023 (DPDP Act). Also 56% do not know their data rights, and 69% do not know they can withdraw their consent.[3]

Cyber security measures and legal framework seek to prevent cyber-crimes and provide penalties. Cyberspace has created many opportunities for individuals to communicate and collaborate across national borders. However, these opportunities have also created new challenges, including phishing and ransomware. Those challenges can come in the form of phishing and ransomware, there was a case of ransomware that happened with AIIMS Delhi

[1] Adversarial Threat Report, First Half 2026 (2026) Zscaler, Inc.,

[2] Reliance Jio commercially launched on 5 September 2016 under a "Welcome Offer" providing free services until 31 December 2016, later extended and rebranded the "Happy New Year Offer" through 31 March 2017. *See* Jio's Journey: Free Data, Free Voice and One Year of Disruptive Offers, India.com (Sept. 5, 2017), https://www.india.com/business/jios-journey-free-data-free-voice-and-one-year-of-disruptive-offers-2450256/; Telecom stocks tumble after RJio extends free services, Bus. Standard (Dec. 1, 2016), https://www.business-standard.com/amp/article/pti-stories/telecom-stocks-tumble-after-rjio-extends-free-services-116120100876_1.html.(last visited Aug. 28, 2026)

[3] PwC India, How Aware and Prepared Are Indian Consumers and Businesses to Navigate the New Era of Digital Privacy? A Survey of India's Data Privacy Landscape (Oct. 22, 2024), https://www.pwc.in/press-releases/2024/only-16-consumers-in-india-understand-the-digital-personal-data-protection-dpdp-act-only-9-indian-organisations-report-a-comprehensive-understanding-of-the-act-pwc-india-survey.html.(last visited Aug. 28, 2026)

which we will discuss below.[4] Cybercrime can affect individuals from anywhere in the world and is not limited to the country in which the victim resides.

LITERATURE REVIEW

Two kinds of sources shape the discussion below: government material explaining how the state has responded to digital arrest fraud, and press reports documenting individual cases in enough detail to show how the scam actually plays out on the ground.

A Press Information Bureau release from the Ministry of Home Affairs lays out what the Centre has done so far — setting up the Indian Cyber Crime Coordination Centre (I4C) as the nodal agency for cybercrime, running an awareness campaign through newspapers, metro announcements and Prasar Bharti, and blocking over 1,700 Skype IDs and nearly 59,000 WhatsApp accounts tied to these scams. The same release points to the Citizen Financial Cyber Fraud Reporting and Management System, which has apparently helped recover more than ₹3,431 crore across close to 9.94 lakh complaints since 2021, with the 1930 helpline as the main entry point for victims.[5] A more recent PIB fact-check, covered by Bharat Express, deals with a forged I4C letter circulating online — fake letterhead, threats of arrest within 24 hours — and places it against a backdrop of losses crossing ₹100 crore nationally in early 2026. It's a small example, but it shows the fraud isn't static; the impersonation tactics are getting more elaborate even as the government pushes back.[6]

The case reporting fills in what the government releases leave abstract. An ORF piece from mid-2026 notes that victims range from senior officials to elderly citizens with limited digital literacy, and gives the example of an elderly man in Mangaluru who lost ₹2.07 crore in April 2026 to callers posing as investigators.[7] A Gulf News report on an 80-year-old retired Delhi

[4] The All India Institute of Medical Sciences, New Delhi, suffered a ransomware attack on 23 November 2022 that encrypted hospital servers and disrupted patient services for roughly a week to ten days. *See* Ransomware Attack at AIIMS: NIA Suspects Cyberterrorism, TAC Security (Nov. 30, 2022), https://tacsecurity.com/ransomware-attack-at-aiims-nia-suspects-cyberterrorism/; AIIMS Cyberattack 2022: Shielding India's Healthcare, AceCloud (Apr. 24, 2025), https://www.acecloudhosting.com/blog/aiims-cyberattack-2022/.(last visited Aug. 28, 2026)

[5] Press Release, Press Information Bureau, Ministry of Home Affairs, *Digital Arrest Scam* (2024), https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2082761&reg=48&lang=2 (last visited Sept. 4, 2026).

[6] *PIB Fact Check Debunks Fabricated I4C Letter Fuelling Digital Arrest Scam*, Bharat Express (Feb. 28, 2026), https://english.bharatexpress.com/fact-check/pib-fact-check-debunks-fabricated-i4c-letter-fuelling-digital-arrest-scam-257467 (last visited Sept. 4, 2026).

[7] *Digital Arrest Scams and the Limits of Domestic Enforcement*, Observer Research Foundation (Jul. 18, 2026), https://www.orfonline.org/expert-speak/digital-arrest-scams-and-the-limits-of-domestic-enforcement (last visited Sept. 4, 2026).

government employee is more granular: fraudsters posing as ED and CBI officials kept him on a continuous video call and had him write out "clarification letters" while they emptied his account; police later found the money had passed through an "account provider" who rented out his bank details for ₹10,000 a pop.[8] This Tribune's report on an 82-year-old woman in Chandigarh covers similar ground from a different angle: forged Supreme Court documents, a fake arrest warrant tying her to a money-laundering case, pressure to move funds into a secure government account.[9]

METHODOLOGY

This research employs a non-empirical, qualitative legal research methodology utilizing a doctrinal approach to examine the legal frameworks and cyber vulnerabilities that target senior citizens whose vulnerability is increased with technological advancement. Doctrinal legal research involves the systematic examination of primary legal materials to determine how the existing legal framework addresses contemporary challenges.

Secondary sources consist of statistical reports and empirical surveys from organizations such as META's adversarial threat report and Zscaler ThreatlaBZ and PWC survey on Indian data privacy. This focuses on helping understand the exploitation of people and low public awareness regarding these phishing and Digital arrest cases that are happening these days. In between 2013 and 14 there was a case where the data of approximately three billion users the data of approximately three billion users was breached who were all yahoo users and it was disclosed by yahoo in 2016.[10] There was a case regarding Digital arrest where an old couple in Faridabad NIT couple were defrauded of rupees 30.2 lakhs, it was a three-day Digital arrest.[11] United States vs Ivanov (2001).[12] This research draws upon primary legal research and commentaries so that with this multidimensional approach potential answers can be

---

[8] *Elderly Delhi Man Loses Rs4.2m in 'Digital Arrest' Scam*, Gulf News, https://gulfnews.com/world/asia/india/elderly-delhi-man-loses-rs4-2m-in-digital-arrest-scam-1.500297795 (last visited Sept. 4, 2026).

[9] *Chandigarh's Elderly Woman Loses Rs 2.5 Crore in Digital Arrest Fraud*, The Tribune, https://www.tribuneindia.com/news/chandigarh/sector-10-elderly-woman-loses-2-5-crore-in-digital-arrest-fraud (last visited Sept. 4, 2026).

[10]. Press Release, U.S. Dep't of Justice, U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts (Mar. 15, 2017), https://www.justice.gov/archives/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.(last visited Aug. 28, 2026)

[11] (I found, e.g., *Elderly couple loses Rs 30L in digital arrest scam*, The Tribune, https://www.tribuneindia.com/news/haryana/elderly-couple-loses-30l-in-digital-arrest-scam/ (last visited Aug. 28, 2026)

[12] United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001)

found. There's also a comparative legal analysis between India and EU and the United States where the EU's GDPR has a robust control over the EU but not outside of it whereas the US has the US CLOUD where it has extraterritorial reach.[13]

THE CHANGING DYNAMICS OF ELDER TARGETED FINANCIAL FRAUD

In recent years, financial fraud targeting elderly persons has become increasingly sophisticated. Traditional scams, such as lottery-related fraud, have increasingly been replaced or supplemented by technology-enabled fraud or digital fraud, including digital arrest scams.[14] In modern age it has transitioned to Digital arrest scams with con causing fraud to the innocent people wherein the criminal impersonates a law enforcement officer.[15] They impersonate a central bureau investigating officer or a policeman or even a judicial officer.[16] According to police officials such acts are targeted mainly towards the elderly persons.[17] This scam has a similar architecture in all of the cases which have previously happened: a person impersonating as a police officer and another officer also in uniform join the video call and then with fake seals and forged documents victims are instructed to isolate themselves from the family, in some cases video calls have lasted several days.[18] Then the victims are asked to transfer funds to some mule accounts and then they are dispersed

[13] Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, div. V, 132 Stat. 348, 1213–25 (2018) (codified as amended in scattered sections of 18 U.S.C.)
[14] *See* Press Release, Press Information Bureau, Ministry of Home Affairs, *Digital Arrest Scam* (2024), https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2082761&reg=48&lang=2 (last visited Sept. 3, 2026).
[15] *MHA Warns of Rising 'Digital Arrest' Scams by Fraudsters Impersonating Govt Officials*, Morung Express (May 15, 2024), https://morungexpress.com/mha-warns-of-rising-digital-arrest-scams-by-fraudsters-impersonating-govt-officials (last visited Sept. 3, 2026).
[16] *India Warns of Rising 'Digital Arrest' Scams by Cybercriminals Impersonating Govt Officials*, Gulf News (2024), https://gulfnews.com/world/asia/india/india-warns-of-rising-digital-arrest-scams-by-cybercriminals-impersonating-govt-official-1.1715689619527 (last visited Sept. 3, 2026).
[17] *Elderly Doctor Couple Kept Under 'Digital Arrest' for Over Two Weeks in Delhi; Duped of Rs 14 Crore*, Deccan Herald, https://www.deccanherald.com/india/delhi/elderly-doctor-couple-kept-under-digital-arrest-for-over-two-weeks-in-delhi-duped-of-rs-14-crore-3858119 https://www.deccanherald.com/amp/story/india%2Fkarnataka%2Felderly-woman-falls-prey-to-digital-arrest-loses-rs-3-09-cr-3674822 (last visited Sept. 3, 2026).
[18] *Amid Rise in Digital Arrest Cases, Indian Cyber Crime Coordination Centre Issues Advisory for Citizens*, Deccan Herald, https://www.deccanherald.com/india/amid-rise-in-digital-arrest-cases-indian-cyber-crime-coordination-centre-issues-advisory-for-citizens-3221509 (last visited Sept. 3, 2026).

therefore making it difficult for the police to track them.[19] With these types of scams people's hard-earned money has been stolen in crores of rupees.[20]

Beyond Digital arrest there are other types of scams where elderly people are asked their OTP, Credit card details and other banking related details and this type of detail gives scammers access to their device. This defeats the trust that elderly people have in security of the bank but rather they are the ones that give access to their device to their scammers unbeknownst to them and their retirement money will go to the scammers.

EXAMINING THE EXISTING LEGAL FRAMEWORK

India has no single statute that has a law of addressing the protection of senior citizens from cyber crimes. Instead it is mentioned in other laws which covers every type of population under one law of land.

Information and Technology Act 2000

Some of the cases involved under this act includes section 66d which has phishing indirectly mentioned with the example of "cheating by personation" where a person who falsely identifies as a policeman or a CBI inspector. The scam generally involves four stages:

1. Bait: The scammer impersonates an authority figure and contacts the victim through a telephone or video call. Senior citizens may be particularly vulnerable because of limited familiarity with digital technology. The scammer creates an appearance of authenticity and attempts to create fear and confusion.
2. The hook: The scammer creates a sense of urgency by informing the victim that a family member has been involved in a serious offence or that the victim is under investigation.

[19] *Elderly Delhi Man Loses Rs4.2m in 'Digital Arrest' Scam*, Gulf News, https://gulfnews.com/world/asia/india/elderly-delhi-man-loses-rs4-2m-in-digital-arrest-scam-1.500297795 (last visited Sept. 3, 2026).

[20] *See* Press Release, Press Information Bureau, *supra* note 1 (financial amount exceeding Rs. 3431 crore saved in over 9.94 lakh complaints registered through the Citizen Financial Cyber Fraud Reporting and Management System); *see also PIB Fact Check Debunks Fabricated I4C Letter Fuelling Digital Arrest Scam*, Bharat Express (Feb. 28, 2026), https://english.bharatexpress.com/fact-check/pib-fact-check-debunks-fabricated-i4c-letter-fuelling-digital-arrest-scam-257467 (last visited Sept. 3, 2026) (reporting financial losses from digital arrest scams exceeding Rs. 100 crore nationwide in early 2026).

3. Digital custody The scammers may continue the video call for several hours and falsely claim that the victim is under surveillance or that the matter involves national security.
4. Financial extraction The scammers then demand money by falsely claiming that the victim must deposit funds into a government-monitored account or pay bail to resolve the alleged investigation.[21]

The sections 66C and 66D of Information Technology Act of 2000 punish anyone who under false pretense uses someone else's identity or personation of another person typically officer of law and when someone fraudulently uses other persons passwords, Digital signature or identification feature through computer source, with imprisonment of three years.[22] These provisions provide protection to victims regardless of their age. However, their effectiveness depends heavily on the victim's ability to identify the offence and report it promptly. This may be particularly difficult for senior citizens with limited digital literacy upon the affected be it senior citizens promptly to identify and report theft- precisely to the point where the elderly are likely to falter.

Maintenance and Welfare of Parents and Senior Citizens Act 2007

Even though this Act is especially for the Senior Citizens, it does not provide a specific legal mechanism for protecting senior citizens from technology-enabled financial fraud; instead this act solely focuses on maintenance of the property they have and are also empowered to order maintenance from relatives. The Act was enacted before the widespread adoption of modern digital financial services and has a very big gap where it leaves the elderly completely helpless in terms of technological literacy.

A separate revision effective from 1 January 2027 introduces the concept of a fraudulent electronic banking transaction. It includes transactions carried out under coercion or duress. This may help address situations such as digital arrest scams, where victims technically authorise transactions because they are acting under pressure.[23]

Digital Personal and Data Protection Act, 2023

---

[21] Information Technology Act, No. 21 of 2000, § 66D (India).
[22] Information Technology Act, No. 21 of 2000, §§ 66C–66D (India)
[23] Reserve Bank of India, Reserve Bank of India (Commercial Banks – Responsible Business Conduct) Directions, 2025 (Amendment) The Policy Edge (June 25, 2026); RBI Caps Customer Liability in Digital Fraud From2027,MediaNama(June25,2026),https://www.medianama.com/2026/06/223-rbi-final-amendment-directions-limiting-customer-liability-digital-transactions-effect-2027/(last visited Aug. 28, 2026)

It focuses on protecting the data of an individual residing in India when, where, and how their data is being used, shared, sold, collected, processed, shared or otherwise used.

- Individuals have the Right to correct their information
- Individuals have the right to request the erasure of their personal information
- Individuals have the Right to access their personal information

It helps in making it mandatory for the companies by the government to secure the data strictly. It is very similar to GDPR. It is the same law that helps the people in the EU having a safeguard and a redressal point where they can request or correct or erase their data.[24]

Some criticism that DPDPA faces are as follows:

1. Broad government exemptions: the central government can exempt state governments under vague blankets like "sovereignty", "state security" and "public order".
2. Missing portability and deletion protections: the act completely omits the standard right to port your data (from one app to another to a competitor) and lacks a true right to be forgotten.[25]

INTERNATIONAL CYBER SECURITY LAWS CONVENTION

The Budapest Convention, 2001, focuses on cross-border cooperation and establishes mechanisms for international assistance, including a 24/7 network of contact points for emergency assistance and a 24/7 network of contact points for emergency mutual help. It is the very first treaty to be signed internationally and binding also addressing computer-related crimes. It was enforced on 1st July 2004. It serves as the primary framework to protect cross-border data.[26]

Malabo Convention, 2014: The Malabo Convention is a convention concerning cybersecurity and data protection in African countries. It focuses on establishing legal frameworks for cybersecurity and data protection.[27]

[24] Digital Personal Data Protection Act, No. 22 of 2023, §§ 11–13 (India)
[25] PRS Legislative Research, The Digital Personal Data Protection Bill, 2023 (2023), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (last visited Aug. 28, 2026)
[26] Convention on Cybercrime, opened for signature Nov. 23, 2001, C.E.T.S. No. 185, entered into force July 1, 2004.
[27] Convention on Cybercrime, opened for signature Nov. 23, 2001, C.E.T.S. No. 185, entered into force July 1, 2004.

United States (state level) – California consumer privacy act: it is the most robust state level protection and privacy law in the United States which helps the people of California in granting the right to know how, when and where their data is being used. The Act was signed into law on 28 June 2018 and came into force on 1 January 2020. Individuals may also request the deletion of their personal information, subject to certain exceptions. They may also have the right to opt out of certain uses of their personal information. They also have a right to opt out of it.[28]

General data protection regulation (GDPR): It was first proposed on January 25th, 2012 and entered into force May 24th, 2016 It is one of the most comprehensive data protection frameworks in the world. It applies to anyone who wants to process inside Europe. Individuals can ask to port their data from one provider to another. They can also ask for their data to be deleted and If their personal data is inaccurate, they may request its correction and can also demand a full copy of their data that the company holds on them. Its key objectives are giving citizens control over their data, simplifying and unifying the digital market and modernizing law for the modern internet.[29]

COMPARATIVE PERSPECTIVE

United States: Decentralized and Sector-Specific Approach

There is no single comprehensive cyber law; instead they rely on different laws like Computer Fraud and Abuse Act (CFAA) for hacking, Electronics Communication Privacy Act (ECPA), and sector-specific rules like HIPAA (health).[30]

Its enforcement and oversight spreads across various law enforcement agencies like FBI, CISA, FTC and state level privacy statutes like California's CCPA.

Intermediary liability: Section 230 proactively appreciates individual control so that it allows more freedom rather than state censorship over it and shield from user generated content.[31]

---

[28] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100–1798.199.100 (signed into law June 28, 2018, effective Jan. 1, 2020).
[29] Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [GDPR] (first proposed by the European Commission Jan. 25, 2012; adopted Apr. 14, 2016; entered into force May 24, 2016.
[30] Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2523; Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936
[31] Communications Decency Act, 47 U.S.C. § 230.

Commercial flexibility: Robust constitutional protection (under fourth amendment) against unreasonable searches and protects public private intelligence sharing.[32]

France and the European Union: An Integrated and Sovereignty-Focused Approach

France's data protection framework is based on its national data protection legislation and is harmonised with the European Union's General Data Protection Regulation and the NIS2 Directive. It was modified in 1978 and fully harmonized with the EU's general data protection regulation and NIS2 directive for network security. [33]

Enforcement and oversight: It is regulated nationally by CNIL (data protection authority) and ANSSI (national cyber security agency).[34]

Intermediary liability bound by Directive Security Act (DSA) helps in removal of online content, mainly consisting of illegal contents eventually leading to instant removal.[35]

Key focus emphasizes privacy digital act and consumer protection and helps in building Europe digital infrastructure independent of foreign infrastructure.

Synthesis: Existing Gaps in India framework

Absence of Demographic-Specific Equity Provisions: There are no enhanced penalties for targeting specific individuals where they give separate penalties to the wrongdoers if they target specific vulnerable groups which consist of senior citizens through grooming or pension-related scams.[36]

Unrecognized Digital Modality: Digital arrest scams may involve criminals intimidating senior citizens into transferring their life savings to accounts controlled by the offenders.

Inadequate Victim Compensation Execution: Civil and criminal provisions place a heavy burden on the victims under section 43A and 66 of the IT ACT where they have to prove specific Mens Rea, (fraudulent intent) and trading life channels where they have to provide financial trading channels resulting in slow resolution times that fail to provide solution for elderly citizens.

---

[32] U.S. Const. amend. IV.

[33] Directive 2022/2555, 2022 O.J. (L 333) 80 (EU) [NIS2 Directive] (entered into force Jan. 16, 2023; member-state transposition deadline Oct. 17, 2024).

[34] Comm'n Nationale de l'Informatique et des Libertés (CNIL), https://www.cnil.fr; Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), https://www.ssi.gouv.fr.(last visited Aug. 28, 2026)

[35] Regulation 2022/2065, 2022 O.J. (L 277) 1 (EU) [Digital Services Act] (entered into force Nov. 16, 2022; applicable Feb. 17, 2024).

[36] Elder Abuse Prevention and Prosecution Act, Pub. L. No. 115-70, 131 Stat. 1208 (2017) (codified as amended in scattered sections of 18 & 42 U.S.C.)

Complex Procedural Hurdle: Mechanisms such as the National Cyber Crime Reporting Portal are there but for senior citizens who may not be technologically well equipped may face hurdles especially where it might require digital evidence mapping, technical navigation, documentation clarity which heavily disfavor elderly.

Investigative Capacity Gap: Local police units frequently lack specialized digital forensics capacity and basic training required to manage senior complainants leading to high case dropouts and lesser stolen funds returned.

YAHOO DATA BREACH (2013-2014)

The breach affected approximately three billion user accounts. The United States Department of Justice later indicted individuals associated with the Russian Federal Security Service (FSB) and criminal hackers in connection with the breach by two Russian FSB (federal security service) and two criminal hackers (including alexsey belan). Their indictment was announced by the US Department of Justice in March 2017. The compromised information included sensitive personal data associated with the user account, but yahoo publicly acknowledged the breach on 22nd, September 2016. This yahoo data breach is considered as the biggest data hack in all of history compromising every user that existed at that time of 3 billion users.

DISCUSSION

The findings of this study demonstrates how technological developments have created new methods of financial fraud targeting senior citizens. The expansion of online banking and UPI has created new opportunities for financial fraud. Senior citizens may be particularly vulnerable because some may have limited digital literacy and may not know when or where to report cybercrime. The development of digital financial services has therefore not always been accompanied by adequate safeguards for vulnerable groups.

A key finding of this study is that the Information Technology Act, 2000 provides a broad legal framework through provisions such as Sections 66C and 66D. However, it does not specifically address the vulnerabilities of senior citizens. Enforcement also depends heavily on timely reporting and preservation of digital evidence, which may be difficult for senior citizens with limited digital literacy or delayed awareness of the fraud.

The study also highlights gaps in the protection provided against technology-enabled or digital financial fraud. The RBI's 2017 circular on customer liability represented an important development by limiting the financial burden on customers in cases of unauthorised electronic transactions. Additional safeguards, including cooling-off periods, emergency account controls, transaction limits and trusted-contact mechanisms, may further strengthen protection. However, several of these measures remain at the advisory or implementation stage, creating a gap between regulatory proposals and effective protection

Overall, this study demonstrates that India's legal framework remains fragmented. Existing measures are largely precautionary or preventive and do not provide a unified age-specific approach to protecting senior citizens. Addressing these gaps requires a victim-centred regulatory model that provides rapid responses and effective financial restitution. This is particularly important because technology-enabled financial fraud can result in the rapid movement of funds across multiple accounts. Such reforms are necessary to ensure that technological advancement does not compromise the financial security and dignity of senior citizens

CONCLUSION

The RBI's regulatory measures introduced in 2017 concerning cooling-off periods, transaction limits and customer liability represent a positive development in the protection of vulnerable persons and senior citizens. Sections 66C and 66D of the Information Technology Act, 2000 provide protection against identity theft and cheating by personation. However, these provisions apply to the general population and do not specifically address the needs of senior citizens. Although the DPDP Act contains certain features similar to the GDPR, questions remain regarding government exemptions and the absence of certain data rights

The United States' sectoral model demonstrates that targeted legal protections can be introduced without a single comprehensive cybercrime statute. Laws such as the CFAA and the California Consumer Privacy Act demonstrate the possibility of targeted legal protections for specific groups. The EU's GDPR and NIS2 framework also demonstrates how data protection, cybersecurity and citizen protection can operate within an integrated regulatory structure. In contrast, India's framework remains fragmented across different statutes, leaving gaps between data protection, cybercrime and consumer protection.

Going forward, India should consider developing a targeted set of rules specifically designed to protect senior citizens and other vulnerable groups. Such rules should not assume a high level of digital literacy. Given that digital arrest scams and mule accounts can result in the rapid transfer of funds, the current emphasis on post-crime criminal enforcement may not adequately address the speed of financial harm. Unless Indian law recognises senior citizens as a category requiring tailored legal protection, technological advancement may continue to outpace the safeguards designed to protect them