

# Victim Support, Rehabilitation and Access to Justice for Elderly Women in the Digital Era: A Critical Study of Legal Protection in India

Julimol P. R<sup>1</sup>, Dr. Sanjaya Choudhury<sup>2</sup>

<sup>1</sup>Ph.D. Research Scholar, Department of Law, Bhagwant University, Ajmer, Rajasthan, India – 305 004

<sup>2</sup>LL.M., Ph.D., Professor of Law, Department of Law, Bhagwant University, Ajmer, Rajasthan, India – 305 004

## Abstract

The rapid expansion of digital technologies has transformed communication, financial transactions, access to public services, and social interaction, while simultaneously creating new forms of vulnerability for elderly women. As increasing numbers of senior women engage with digital platforms, online banking, social media, and digital government services, they are exposed to cyber fraud, identity theft, financial exploitation, online harassment, privacy violations, impersonation, and technology-facilitated abuse. These emerging forms of victimisation often intersect with age, gender, economic dependency, social isolation, and limited digital literacy, thereby creating significant barriers to effective access to justice.

This paper critically examines the adequacy of the existing Indian legal framework for protecting elderly women from digital and technology-facilitated offences, with particular emphasis on victim support, rehabilitation, and access to justice. It analyses the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023 and its phased implementation framework, the Maintenance and Welfare of Parents and Senior Citizens Act, 2007, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Legal Services Authorities Act, 1987, and institutional mechanisms such as the National Cyber Crime Reporting Portal, the Indian Cyber Crime Coordination Centre and legal services authorities. It also considers the constitutional foundations of dignity, equality, privacy and access to justice.

The paper identifies underreporting, lack of awareness, difficulties in navigating digital complaint mechanisms, evidentiary challenges, delays in investigation, fragmented institutional responsibility, and limited access to specialised victim-support services as significant barriers. It argues that criminalisation alone is insufficient. Legal protection must move towards a victim-centred framework integrating prevention, accessible reporting, legal assistance, psychological and social support, financial recovery, rehabilitation, digital literacy and platform accountability. The paper proposes an age- and gender-sensitive cyber justice model based on early intervention, coordinated institutional response, accessible remedies and meaningful participation of elderly women in the justice process.

**Keywords:** Elderly Women; Digital Era; Cybercrime; Victim Support; Rehabilitation; Access to Justice; Legal Protection; Digital Literacy; Privacy; Financial Exploitation.

## 1. Introduction

Digitalization has become an essential component of everyday life in India. Banking, payments, healthcare, public welfare, education, communication, travel and government services are increasingly accessed through digital platforms. This transformation has brought considerable benefits to older persons by reducing physical barriers and improving access to services. At the same time, digital dependence can create a new field of victimisation for persons who have limited experience with rapidly changing technologies. Elderly women may face a particularly complex form of vulnerability because age-related barriers may overlap with gender inequality, widowhood, economic dependence, social isolation, limited property ownership, lack of digital confidence and dependence upon family members or intermediaries.

The India Ageing Report 2023 has highlighted digital ignorance and the challenge of enabling senior citizens to use digital platforms as important concerns in an ageing society. It also draws attention to the gendered character of poverty in old age and the greater likelihood of older women being widowed, living alone or lacking independent income and assets.<sup>1</sup> The significance of these factors in the digital environment is substantial: a person who depends upon another individual to operate a mobile phone, access online banking, manage passwords or complete a government application may be exposed not only to external cybercriminals but also to exploitation by persons within the circle of trust.

The problem is therefore not simply whether an offence has been criminalised. The deeper question is whether an elderly woman who becomes a victim can understand what happened, report it without fear or technological difficulty, obtain immediate assistance, preserve evidence, recover her money or identity, access legal representation, receive psychological support, and obtain a remedy within a reasonable time. A legal system that punishes the offender but leaves the victim without practical assistance cannot be regarded as fully responsive to the contemporary meaning of access to justice.

The paper proceeds from the proposition that elderly women in the digital era require an intersectional legal response. The categories of 'elderly person' and 'woman' should not operate independently. Their combined effect may produce distinct forms of vulnerability. The appropriate legal framework must therefore be age-sensitive, gender-sensitive, technologically informed and victim-centred.

## 2. Statement of the Problem

The expansion of digital transactions has altered the nature of victimisation. Traditional forms of elder abuse such as physical violence, abandonment, property-related exploitation and financial abuse may now be facilitated through digital technologies. An offender may obtain a victim's banking credentials through deception, impersonate a bank official, induce the victim to disclose an OTP, create a false social-media profile, manipulate a digital identity, threaten publication of private material, or use remote-access technology to control a device. The resulting harm may include financial loss, reputational injury, psychological trauma, loss of privacy and continuing insecurity. The legal response is fragmented across criminal law, cyber law, data protection law, elder-welfare legislation and legal-aid mechanisms. This fragmentation may make the system difficult for an elderly victim to navigate. A victim may not know whether to approach the local police station, cyber police station, bank, cybercrime portal, District Legal Services Authority, senior-

---

<sup>1</sup> UNFPA India and International Institute for Population Sciences, Caring for Our Elders: Institutional Responses – India Ageing Report 2023 (2023); Government of India, Ministry of Social Justice and Empowerment, 'India Ageing Report-2023', PIB, 6 February 2024.

citizen authority or another institution. The first few hours after a financial cyber fraud can also be crucial for attempting to freeze or trace the transaction. Consequently, accessibility and speed are themselves dimensions of justice.

The problem is further aggravated by underreporting. Elderly women may hesitate to disclose victimization because of shame, fear of losing family support, fear of being considered digitally incompetent, dependence upon the accused, or the belief that recovery is impossible. When the offender is a relative, caregiver or trusted intermediary, the victim may be especially reluctant to initiate criminal proceedings.

### 3. Objectives of the Study

- To examine the forms of digital and technology-facilitated victimisation experienced by elderly women.
- To analyse the constitutional and statutory framework protecting elderly women in India.
- To examine the adequacy of cybercrime reporting, investigation, compensation and legal-aid mechanisms.
- To identify barriers affecting reporting, evidence, investigation, recovery and rehabilitation.
- To develop recommendations for an age-sensitive and gender-responsive victim-centred framework.

### 4. Research Questions

1. Are existing Indian criminal and cyber laws adequate to protect elderly women from digital victimization?
2. How effectively do present mechanisms provide victim support, compensation and rehabilitation?
3. What procedural and institutional barriers prevent elderly women from accessing justice?
4. What reforms are necessary to create a rights-based, accessible and technologically responsive justice framework?

### 5. Research Methodology

The study adopts a doctrinal and analytical legal research methodology. Primary legal materials include the Constitution of India, statutes, delegated legislation and judicial decisions. Secondary materials include government reports, official institutional information, international human-rights principles and scholarly literature. The analysis is primarily qualitative and focuses on the relationship between substantive criminal law, procedural remedies, data protection, elder welfare, legal aid and institutional response. The study does not claim to present original empirical survey data; where statistical or institutional information is used, it is drawn from identified government or intergovernmental sources.

### 6. Conceptualising the Vulnerability of Elderly Women in the Digital Era

Vulnerability should not be treated as an inherent characteristic of old age. Older persons are diverse, capable and entitled to autonomy. The United Nations Principles for Older Persons emphasize independence, participation, care, self-fulfillment and dignity, including the right of older persons to access social and legal services and to live free from exploitation and abuse<sup>2</sup>. The appropriate legal

---

<sup>2</sup> United Nations General Assembly, United Nations Principles for Older Persons, GA Res 46/91, 16 December 1991, principles 12, 13, 14 and 17.

approach is therefore not to exclude elderly women from digital participation but to make digital participation safe, accessible and meaningful.

Elderly women may experience multiple and overlapping vulnerabilities. First, age may be associated with lower familiarity with cybersecurity practices, changing interfaces and new forms of fraud. Second, gender inequality may affect control over property, financial resources and technology. Third, widowhood or living alone may reduce the availability of trusted assistance. Fourth, economic dependence may make financial loss particularly devastating. Fifth, physical or sensory limitations may make complex digital complaint systems difficult to use. Sixth, social isolation may increase exposure to fraudulent relationships, impersonation and online manipulation.

This intersectional vulnerability has important legal consequences. A universal cybercrime framework assumes that every victim possesses comparable digital literacy, confidence and resources. That assumption is unrealistic. Equality in access to justice sometimes requires differentiated assistance. An elderly woman who cannot navigate an online complaint form may require assisted reporting rather than simply being directed to a website. Similarly, a victim of financial fraud may need immediate coordination between police, banks and payment intermediaries rather than a conventional complaint process that begins and ends with registration of an FIR.

## **7. Forms of Digital Victimization of Elderly Women**

### **7.1 Cyber Fraud and Financial Exploitation**

Financial cyber fraud is among the most consequential forms of digital victimisation. Fraudsters may impersonate bank officials, government officers, police officers, delivery agents or relatives. Social-engineering techniques may persuade victims to disclose OTPs, PINs, passwords or other credentials. The harm may extend beyond the initial transaction where the victim's account, identity documents or contact information are subsequently misused.

The National Cyber Crime Reporting Portal provides a mechanism for reporting cybercrime and specifically provides a 24-hour helpline, 1930, for immediate reporting of cyber financial fraud.<sup>3</sup> the importance of rapid reporting is considerable because early intervention may create opportunities for tracing or placing holds on fraudulent transfers. Nevertheless, the existence of a portal does not by itself guarantee access to justice. An elderly victim may need assisted filing, language support and guidance regarding the evidence to preserve.

### **7.2 Identity Theft and Impersonation**

Identity theft can involve misuse of passwords, electronic signatures, account credentials or other identifying information. Section 66C of the Information Technology Act, 2000 addresses identity theft, while section 66D addresses cheating by personation using a computer resource or communication device.<sup>4</sup> The Bharatiya Nyaya Sanhita, 2023 also contains provisions concerning cheating and cheating by personation.<sup>5</sup> The parallel operation of general criminal law and special cyber law can provide legal coverage, but victims and investigators must be able to identify the appropriate provisions and preserve the electronic evidence necessary to establish the offence.

<sup>3</sup> Indian Cyber Crime Coordination Centre, National Cyber Crime Reporting Portal, Government of India, including the 24x7 cyber financial fraud helpline 1930.

<sup>4</sup> Information Technology Act, 2000, ss 66C and 66D.

<sup>5</sup> Bharatiya Nyaya Sanhita, 2023, provisions relating to cheating and cheating by personation.

### 7.3 Privacy Violations and Technology-Facilitated Harassment

Elderly women may experience online harassment, unauthorised disclosure of personal information, impersonation, stalking-like conduct, threats and misuse of private images or communications. Privacy is constitutionally protected as part of the right to life and personal liberty. In *K.S. Puttaswamy v Union of India*<sup>6</sup>, the Supreme Court recognised privacy as a constitutionally protected right. In the digital context, privacy protection is closely connected to dignity because exposure of financial, medical, family or identity information can produce continuing harm even after a criminal act has ended.

### 7.4 Abuse by Persons in a Position of Trust

Digital abuse may be perpetrated by caregivers, relatives, domestic workers, financial intermediaries or other trusted persons. Such persons may have direct access to phones, passwords, bank applications, documents or government accounts. The problem therefore intersects with the broader concept of elder abuse. The Maintenance and Welfare of Parents and Senior Citizens Act, 2007 contains provisions dealing with protection of life and property, awareness, coordination and abandonment.<sup>7</sup> Its framework is particularly relevant where digital exploitation is accompanied by broader financial or familial abuse.

## 8. Constitutional Foundations of Protection

The constitutional framework provides a normative foundation for protecting elderly women from digital victimisation. Article 14 guarantees equality before the law and equal protection of the laws. Article 15 prohibits discrimination on specified grounds, including sex. Article 21 protects life and personal liberty and has been interpreted to include dignity, privacy and meaningful conditions of life. Article 39(e) and (f) and Article 41 reflect the constitutional commitment to social protection and assistance, although the Directive Principles operate differently from enforceable fundamental rights.

The Supreme Court's jurisprudence concerning older persons reinforces the importance of dignity. In *Dr Ashwani Kumar v Union of India*, the Court considered the rights of elderly persons under Article 21 and emphasised the constitutional significance of dignity, shelter and health, while directing attention to effective implementation of the senior-citizen welfare framework.<sup>8</sup> The decision is important for the present study because it demonstrates that protection of older persons is not merely a matter of charity or welfare administration; it has a constitutional dimension.

Gender-sensitive interpretation is equally important. In *Anuj Garg v Hotel Association of India*, the Supreme Court rejected protective approaches based on gender stereotypes and emphasised that law should not perpetuate the oppression it claims to prevent.<sup>9</sup> Applied to elderly women, this principle suggests that protection should strengthen autonomy and agency rather than treat women as passive recipients of paternalistic assistance.

## 9. Criminal Law Framework

The Bharatiya Nyaya Sanhita, 2023 replaced the Indian Penal Code as the principal substantive criminal law from 1 July 2024. Its provisions on cheating and cheating by personation can apply to technology-facilitated fraud depending on the facts.<sup>10</sup> The Information Technology Act, 2000 continues to provide

<sup>6</sup> *K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1.

<sup>7</sup> Maintenance and Welfare of Parents and Senior Citizens Act, 2007, particularly ss 20–25 concerning medical facilities, awareness, protection of life and property, and abandonment.

<sup>8</sup> *Dr Ashwani Kumar v Union of India*, 2018 INSC 1201 (Supreme Court of India, 13 December 2018).

<sup>9</sup> *Anuj Garg v Hotel Association of India*, (2008) 3 SCC 1

<sup>10</sup> Bharatiya Nyaya Sanhita, 2023, s 318 (cheating) and s 319 (cheating by personation).

offence-specific provisions relevant to cyber conduct, including identity theft under section 66C and cheating by personation using computer resources under section 66D.

The coexistence of general criminal law and cyber-specific provisions is not inherently problematic. It allows investigators to characterise conduct according to its substantive harm and technological method. However, practical difficulties arise when victims or first responders do not understand the interaction between the laws. A victim-centred system should therefore place the burden of legal classification on trained investigators and prosecutors rather than on the victim.

Criminal law also needs to be evaluated by its capacity to address victim recovery. Imprisonment and fines primarily operate against offenders. They do not automatically restore money, repair credit or identity damage, provide counselling or address the victim's fear of future victimisation. Consequently, substantive criminalisation must be complemented by procedural and welfare measures.

### **10. Information Technology Act, 2000 and Digital Evidence**

The Information Technology Act remains an important component of India's cybercrime framework. Sections 66C and 66D directly address identity theft and personation. Section 43A has also historically provided a compensation mechanism where a body corporate handling sensitive personal data is negligent in implementing reasonable security practices and procedures and such negligence causes wrongful loss or wrongful gain.<sup>11</sup>

The evidentiary dimension is critical. Digital fraud may leave traces in transaction records, call logs, IP information, device identifiers, emails, messages, application logs and bank records. However, elderly victims may delete messages, reset devices or fail to preserve screenshots because they are unfamiliar with evidentiary requirements. Investigators therefore require protocols that enable rapid preservation of digital evidence without placing unrealistic technical responsibilities upon victims.

Training should include not only technical investigation but also victim communication. An elderly complainant should not be made to feel responsible for having been deceived. Such an approach can reinforce shame and discourage future reporting.

### **11. Digital Personal Data Protection Framework<sup>12</sup>**

The Digital Personal Data Protection Act, 2023 establishes a framework governing the processing of digital personal data. It recognises the interest of individuals in protecting personal data while permitting lawful processing.

The framework is particularly relevant to elderly women because financial, health, identity and contact information can become tools of exploitation when improperly processed, disclosed or secured.

The implementation position requires careful attention. The Digital Personal Data Protection Rules, 2025 were notified in November 2025, with a phased commencement structure. Some provisions took effect immediately, while other substantive obligations are scheduled to commence after one year or eighteen months.<sup>13</sup> Therefore, as of October 2026, not every substantive obligation under the Act and

---

<sup>11</sup> Information Technology Act, 2000, s 43A, as applicable during the phased commencement of the Digital Personal Data Protection framework.

<sup>12</sup> Digital Personal Data Protection Act, 2023, long title and provisions concerning processing of digital personal data and rights and duties of individuals.

<sup>13</sup> Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), 13 November 2025; Digital Personal Data Protection Act commencement notification, G.S.R. 843(E), 13 November 2025. The framework provides phased commencement of provisions.

Rules should be treated as fully operational. Academic analysis should distinguish enacted law from provisions already in force.

The data-protection framework can strengthen prevention by imposing responsibilities on entities that process personal data. Yet elderly victims require more than abstract data rights. Consent notices, grievance systems and privacy controls must be understandable and accessible. An elderly woman should be able to exercise data-related rights through assisted, multilingual and disability-sensitive channels. Digital consent cannot be meaningful where the user does not understand what information is being collected or how it will be used.

### **12. Maintenance and Welfare of Parents and Senior Citizens Act, 2007**

The Maintenance and Welfare of Parents and Senior Citizens Act, 2007 is an important welfare statute for persons aged sixty years and above. Its objectives include maintenance, welfare and protection of life and property. The Act requires measures relating to publicity and awareness and calls for sensitisation and coordination among relevant departments. It also addresses protection of property in specified circumstances and abandonment of senior citizens.

The statute<sup>14</sup> was enacted before the contemporary scale of digital financial services and therefore does not expressly constitute a comprehensive cyber-elder-abuse statute. Nevertheless, its concepts can complement cybercrime law. Digital financial exploitation may be connected with broader property exploitation, coercion, neglect or abuse by persons who owe duties of care. The Act can therefore function as one layer of protection, but it should not be expected to substitute for a dedicated digital-victim support mechanism.

### **13. Procedural Protection and Victim Compensation under BNSS**

The Bharatiya Nagarik Suraksha Sanhita, 2023 contains a significant victim-oriented mechanism in section 396. It provides for State victim compensation schemes for victims or dependents who suffer loss or injury as a result of crime and require rehabilitation. It also permits compensation applications where an offender is not traced or identified, and provides for interim assistance in appropriate circumstances<sup>15</sup>.

This provision has considerable potential for elderly women affected by cyber fraud. Cybercrime cases may involve anonymous or foreign actors, layered transactions and incomplete identification of offenders. A victim should not necessarily be left without a remedy merely because prosecution is delayed or the offender cannot be traced. The rehabilitation orientation of section 396 supports a broader understanding of justice.

However, the practical effectiveness of compensation depends upon awareness, accessible application procedures and adequate state schemes. Elderly women should be able to receive assistance from the District Legal Services Authority or other authorised institutions in preparing and pursuing compensation claims. Compensation should also be understood broadly enough to address financial loss, reasonable support for rehabilitation and associated consequences of victimisation, subject to the governing scheme and legal requirements.

---

<sup>14</sup> Maintenance and Welfare of Parents and Senior Citizens Act, 2007

<sup>15</sup> Bharatiya Nagarik Suraksha Sanhita, 2023, s 396 (Victim Compensation Scheme).

#### **14. Legal Aid and Access to Justice**

Access to justice requires more than physical access to courts. It includes the ability to understand rights, report wrongdoing, obtain legal advice, participate in proceedings, obtain evidence, receive a timely decision and secure an effective remedy. The Legal Services Authorities Act, 1987 provides the statutory basis for legal aid, and NALSA<sup>16</sup> operates schemes and institutional mechanisms for weaker and vulnerable sections. NALSA also maintains a Legal Services to Senior Citizens Scheme.

For elderly women, legal aid should be integrated with digital assistance. A legal-aid clinic could provide a combined service: cybercrime complaint assistance, bank-fraud documentation, evidence preservation, application for compensation, advice concerning senior-citizen welfare rights and referral for counselling. This integrated model would reduce the burden of approaching multiple institutions.

The present availability of the National Cyber Crime Reporting Portal and the 1930 helpline is an important development. Yet digital accessibility must remain a central design concern. A portal is not genuinely accessible merely because it is available online. Accessibility requires simple language, local-language options, readable interfaces, assisted filing, confirmation of complaint status and the ability to communicate with a human support person where necessary.

#### **15. Institutional Mechanisms and Their Limitations**

India has developed several institutions relevant to cyber victimisation, including police cyber cells, the Indian Cyber Crime Coordination Centre, the National Cyber Crime Reporting Portal, forensic laboratories, banks and financial institutions, legal services authorities and senior-citizen welfare authorities. Government information indicates that cybercrime investigation capacity has been strengthened through national cyber forensic facilities<sup>17</sup> and coordination mechanisms.

The principal institutional weakness is not necessarily absence of institutions but fragmentation. A victim may encounter several institutions that each hold only one part of the solution. The police may investigate the offence; the bank may attempt transaction intervention; the cybercrime portal may record the complaint; the legal services authority may provide legal assistance; and a senior-citizen authority may address elder-welfare concerns. Without coordination, the victim becomes the person responsible for moving information between institutions.

A coordinated case-management model would improve outcomes. Once a complaint is identified as involving an elderly woman, a designated nodal officer could coordinate police investigation, financial intervention, evidence preservation, legal aid, compensation and psychosocial support. Such a model would not require creation of an entirely new bureaucracy; it could operate through designated officers and inter-agency protocols.

#### **16. Barriers to Reporting and Access to Justice**

##### **16.1 Digital Literacy and Interface Barriers**

Digital literacy is not simply the ability to use a smartphone. It includes the capacity to recognise deception, understand privacy settings, distinguish legitimate communications from fraudulent ones,

---

<sup>16</sup> The National Legal Services Authority (NALSA) is a statutory body in India, established under the Legal Services Authorities Act, 1987, with the primary objective of providing free legal aid to marginalized and weaker sections of society and ensuring that justice is accessible to all citizens regardless of economic or social constraints.

<sup>17</sup> National Cyber Crime Reporting Portal, Government of India, 'Report Cyber Crime' and 'Financial Fraud' facilities.

preserve evidence and navigate complaint mechanisms. Older persons who are unfamiliar with digital interfaces may be unable to complete multi-step complaint processes without assistance.

### **16.2 Fear, Shame and Social Dependence**

Victims may blame themselves for being deceived. Elderly women may also fear family criticism or loss of independence. Where the offender is a relative or caregiver, reporting may threaten an existing support relationship. Victim-support systems must therefore be confidential, non-judgmental and capable of assessing dependency and risk.

### **16.3 Underreporting and Data Gaps**

The Government has noted that NCRB cybercrime data do not separately identify cybercrime complaints made by elderly persons.<sup>18</sup> This creates an important policy problem. If age- and gender-disaggregated data are not consistently collected, policymakers cannot accurately measure the scale of digital victimisation of elderly women or evaluate targeted interventions. Future crime-data systems should, subject to privacy safeguards, record age, gender, type of cyber offence, financial loss, relationship with the offender, reporting channel and outcome.

### **16.4 Evidentiary Challenges**

Electronic evidence can be volatile and distributed across devices, banks, platforms and service providers. Elderly victims may not know how to preserve it. Police personnel also require continuing training in digital evidence and forensic procedures. A victim-centred protocol should tell the complainant what not to delete and should enable trained officers to secure relevant information quickly.

### **16.5 Delay in Investigation and Recovery**

Delay can transform a recoverable financial loss into a permanent loss. The first-response system should therefore distinguish cyber financial fraud from ordinary complaints requiring lengthy preliminary processes. Immediate reporting to 1930 and coordinated action with financial institutions can be critical.<sup>19</sup>

## **17. Victim Support: From Complaint to Recovery**

Victim support should begin immediately after the complaint and continue beyond the criminal trial. For elderly women, support can be organized into five stages: immediate protection, legal assistance, financial recovery, psychosocial rehabilitation and long-term digital empowerment.

First, immediate protection requires securing accounts, blocking compromised credentials, preventing further contact by offenders and protecting the victim from retaliation. Second, legal assistance requires clear advice on criminal, civil, data-protection and senior-citizen remedies. Third, financial recovery requires rapid communication with banks and payment intermediaries and access to compensation mechanisms where available. Fourth, psychosocial support should address anxiety, shame, fear and loss of confidence. Fifth, rehabilitation should include practical digital literacy and safe-use training.

The objective should not be to remove elderly women from digital life. Such an approach would reproduce exclusion. Instead, rehabilitation should restore confidence and autonomy. Safe digital participation is itself a component of dignity and independence.

<sup>18</sup> Ministry of Home Affairs, Government of India, 'Incidents of Cyber Crime Targeting Elderly People', PIB, 22 July 2025. The Government stated that NCRB does not separately maintain cybercrime complaint data for elderly persons.

<sup>19</sup> National Cyber Crime Reporting Portal, Government of India, guidance concerning immediate reporting of cyber financial fraud through 1930.

### 18. Role of Digital Platforms, Banks and Service Providers

Technology companies and financial institutions occupy an important position in preventing and responding to digital abuse. Their systems can incorporate risk-based warnings, suspicious transaction detection, fraud reporting channels, account recovery mechanisms and accessible customer support. Elderly users should not be forced to navigate complex automated systems when substantial financial harm is suspected.

Financial institutions should develop age-sensitive fraud-prevention communication without stereotyping older customers. Alerts should be clear and actionable. Where a transaction exhibits strong fraud indicators, institutions should have effective mechanisms for temporary review consistent with applicable law and banking regulation.

Digital platforms should also provide accessible mechanisms for reporting impersonation, harassment and fraudulent accounts. Where the victim is an elderly person, platform support should recognise the possibility that the victim may not understand technical terminology. Accountability should include transparent complaint tracking and timely communication.

### 19. Need for an Age- and Gender-Sensitive Cyber Justice Model

The central argument of this paper is that India's cyber justice architecture should explicitly recognise the intersection of age and gender. An elderly woman should not be required to fit herself into either an ordinary cybercrime model or a general senior-citizen welfare model. Her experience may involve both.

An age- and gender-sensitive cyber justice model should contain six elements:

1. Accessible prevention: digital literacy programmes should be designed for older women using local languages, practical examples and repeated training rather than one-time awareness campaigns.
2. Assisted reporting: cybercrime portals and police stations should provide assisted filing, including telephone and in-person support.
3. Rapid financial intervention: complaints involving financial loss should trigger coordinated response with banks and payment intermediaries.
4. Integrated legal aid: legal services authorities should provide combined assistance covering cybercrime, compensation, banking disputes and senior-citizen rights.
5. Rehabilitation: victims should receive counselling, confidence-building and digital safety training.
6. Data-driven policy: government agencies should collect anonymised age- and gender-disaggregated data to identify patterns and evaluate interventions.

### 20. Comparative and International Human-Rights Perspective

The international framework provides a useful normative basis for the proposed model. The United Nations Principles for Older Persons recognise older persons rights to independence, participation, care, self-fulfillment and dignity. They expressly refer to access to social and legal services and freedom from exploitation and abuse. These principles support an approach in which elderly women are treated as rights-holders rather than merely beneficiaries of welfare.

The international human-rights perspective also reinforces the importance of participation. Elderly women should be involved in the design and testing of digital services, complaint systems and awareness programmes. Policies designed without listening to older users may unintentionally reproduce exclusion through complicated interfaces, inaccessible language or assumptions about digital competence.

## 21. Recommendations

- **Create a national protocol for cyber victimisation of senior citizens.** – The protocol should establish standard procedures for first response, evidence preservation, financial intervention, legal aid, compensation and rehabilitation.
- **Establish assisted cybercrime reporting facilities.** – Every district should provide a human-assisted reporting option linked to the National Cyber Crime Reporting Portal and 1930.
- **Develop an elderly-women cyber safety programme.** – Training should cover UPI and banking fraud, OTP and password safety, impersonation, privacy, social-media abuse and evidence preservation.
- **Strengthen age- and gender-disaggregated cybercrime data.** – NCRB and related agencies should consider recording age and gender in cybercrime data while protecting personal privacy.
- **Integrate NALSA and senior-citizen mechanisms.** – District Legal Services Authorities should be linked to cybercrime response so victims can receive legal advice and assistance with compensation.
- **Create a dedicated victim-support referral mechanism.** – Police and cybercrime units should be able to refer elderly women to counselling, social welfare and rehabilitation services.
- **Improve platform and financial-institution accessibility.** – Banks and digital platforms should maintain clear fraud-reporting channels and human escalation pathways for vulnerable users.
- **Train police, prosecutors and judicial officers.** – Training should cover cybercrime, elder abuse, gender sensitivity, digital evidence and trauma-informed communication.
- **Treat digital literacy as a component of rehabilitation.** – Victims should be supported in safely returning to digital services rather than being advised simply to avoid technology.
- **Conduct periodic review of the legal framework.** – The interaction among BNS, BNSS, IT Act, DPDP framework and senior-citizen legislation should be periodically reviewed to address gaps and duplication.

## 22. Conclusion

The digital transformation of Indian society has created opportunities for elderly women to access financial services, communication and public institutions, but it has also created new pathways for exploitation. The legal problem is therefore multidimensional. Cyber fraud may simultaneously constitute a criminal offence, a privacy violation, financial exploitation and an elder-abuse concern. The response cannot be confined to punishment.

India already possesses important legal and institutional building blocks: constitutional protections of equality, dignity and privacy; the Information Technology Act; the Bharatiya Nyaya Sanhita; the Bharatiya Nagarik Suraksha Sanhita and its victim-compensation framework; the Maintenance and Welfare of Parents and Senior Citizens Act; the Digital Personal Data Protection framework; NALSA and legal services institutions; and the National Cyber Crime Reporting Portal. The challenge is to connect these mechanisms around the needs of the victim.

A meaningful access-to-justice model must therefore move from an offender-centred conception of cybercrime towards a victim-centred conception of cyber justice. Elderly women require accessible reporting, immediate financial intervention, legal assistance, privacy protection, evidence support, compensation, psychological care and digital rehabilitation. Such protection should enhance autonomy rather than produce paternalistic exclusion.

The ultimate measure of legal protection is not merely how many offences are registered or how many offenders are prosecuted. It is whether a victim can regain security, dignity, financial stability and confidence after the violation. For elderly women in India's digital era, access to justice must therefore mean not only access to the law, but access to an understandable, responsive and humane system capable of accompanying the victim from the moment of victimisation through recovery and rehabilitation.

**Selected Bibliography**

1. Constitution of India.
2. Bharatiya Nagarik Suraksha Sanhita, 2023.
3. Bharatiya Nyaya Sanhita, 2023.
4. Digital Personal Data Protection Act, 2023.
5. Digital Personal Data Protection Rules, 2025.
6. Information Technology Act, 2000.
7. Legal Services Authorities Act, 1987.
8. Maintenance and Welfare of Parents and Senior Citizens Act, 2007.
9. National Legal Services Authority, NALSA (Legal Services to Senior Citizens) Scheme, 2016.
10. National Cyber Crime Reporting Portal, Government of India.
11. UNFPA India and IIPS, Caring for Our Elders: Institutional Responses – India Ageing Report 2023.
12. United Nations General Assembly, United Nations Principles for Older Persons, GA Res 46/91.
13. K.S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.
14. Anuj Garg v Hotel Association of India, (2008) 3 SCC 1.
15. Dr Ashwani Kumar v Union of India, 2018 INSC 1201.