# Data Privacy, Cybersecurity and Trust: Legal Challenges Faced by Women Entrepreneurs in Adopting Digital Finance in India

Annu Soman, Research Scholar
Dr. Rishi Sharma, HOD, SIRTE
Asha Soman Advocate

**ABSTRACT**

*India's rapid shift towards digital finance has created new opportunities for women entrepreneurs, especially at the micro and small-enterprise level. Tools such as UPI, mobile wallets, internet banking and app-based lending promise faster transactions, improved record-keeping and better access to formal finance. Yet, recent studies show that women continue to lag behind men in the active and confident use of digital financial services, and that concerns about fraud, data misuse and lack of redress strongly influence their behaviour (MicroSave Consulting, 2020; World Bank, 2022).*

*This paper examines the legal challenges faced by women entrepreneurs in adopting digital finance in India, with a particular focus on data privacy, cybersecurity and trust. It outlines the typical ways in which women-led micro and small enterprises engage with digital finance, and then analyses the relevant legal and regulatory framework: the Information Technology Act, 2000; Reserve Bank of India (RBI) directions on digital payments, customer protection and security controls; consumer-protection mechanisms such as the Integrated Ombudsman Scheme; and selected policy initiatives on cybersecurity. Drawing on recent policy reports and empirical studies, the paper argues that although a formal protection architecture exists, its effectiveness is limited by low legal and digital literacy, socio-cultural constraints, complex grievance procedures and limited gender-sensitive design of digital-finance products.*

*The paper concludes that strengthening legal literacy, simplifying redress mechanisms, improving privacy-by-design features and enforcing robust data-protection and security standards are essential steps to build trust and to ensure that digital finance genuinely empowers, rather than exposes, women entrepreneurs in India.*

**Keywords:** women entrepreneurs; digital finance; data privacy; cybersecurity; India

## 1. INTRODUCTION

Digital financial services have expanded rapidly in India in the last decade, driven by the growth of the Unified Payments Interface (UPI), Aadhaar-based authentication, and a vibrant fintech ecosystem. The Global Findex Database 2021 shows that India has made substantial progress in account ownership and digital payments, particularly during the COVID-19 period (World Bank, 2022). Public policy has increasingly promoted digital transactions as a means to deepen financial inclusion and foster entrepreneurship.

Women entrepreneurs have been a specific focus of many inclusion and livelihood programmes. Initiatives targeting self-help groups (SHGs), micro-enterprises and women-owned small businesses encourage the use of digital payments, mobile banking and app-based services to improve business efficiency and to create transaction histories that facilitate access to formal credit (UN Women, 2021). In practice, many women-led enterprises now accept UPI payments through QR codes, use mobile wallets, and rely on internet banking for basic transactions.

However, adoption is uneven and often characterised by hesitation and partial use. Field studies report lower levels of active usage and higher levels of fear among women compared to men when it comes to digital financial services (MicroSave Consulting, 2020; NITI Aayog, 2021). Concerns about fraud, data theft, unauthorised transactions and misuse of personal information are compounded by low digital literacy, shared device usage and socio-cultural norms that limit women's control over financial decisions.

This context raises the central research question for this paper: How adequate are India's legal and regulatory frameworks in protecting women entrepreneurs from data-privacy and cybersecurity risks in digital finance, and how do these protections affect their trust and willingness to adopt such tools?

Beyond the national context, these questions are closely linked to the Sustainable Development Goals (SDGs). Secure and inclusive digital finance for women entrepreneurs is related to SDG 5 (Gender Equality), especially targets on women's economic empowerment and access to financial services; SDG 8 (Decent Work and Economic Growth), which stresses support for micro, small and medium enterprises; and SDG 16 (Peace, Justice and Strong Institutions), which calls for effective, accountable and inclusive institutions and equal access to justice. Strengthening data-privacy, cybersecurity and consumer-protection frameworks for women using digital finance is therefore not only a domestic legal concern but also part of

India's commitments under the 2030 Agenda for Sustainable Development (United Nations, 2015).

The objectives of this paper are threefold:

- To describe the main forms of digital finance used by women entrepreneurs in India and the associated privacy and security concerns.
- To analyse the relevant legal and regulatory framework governing data protection, cybersecurity and consumer protection in the digital-finance space.
- To identify gender-specific gaps in implementation and propose measures to strengthen both legal protection and trust.

The paper adopts a doctrinal and socio-legal approach. It reviews statutory and regulatory instruments—especially the Information Technology Act, 2000, Reserve Bank of India (RBI) directions on digital-payment security and customer protection, the Integrated Ombudsman Scheme, and government cybersecurity initiatives—alongside recent empirical and policy reports (MicroSave Consulting, 2020; NITI Aayog, 2021; UN Women, 2021; World Bank, 2022; Ministry of Electronics and Information Technology (MeitY), 2023).

## 2. DIGITAL FINANCE AND WOMEN ENTREPRENEURS IN INDIA

2.1. **Forms of Digital Finance in Use**: Women entrepreneurs in India, particularly those operating micro and small enterprises, increasingly interact with:

- UPI and QR-code payments through apps such as BHIM, PhonePe, Google Pay and Paytm.
- Mobile wallets and prepaid payment instruments (PPIs) for small-value transactions and bill payments.
- Internet and mobile banking for fund transfers, bill payments and loan repayments.
- Digital-lending and fintech platforms that provide small working-capital loans, often with algorithmic underwriting.
- Digital bookkeeping and inventory-management apps that record sales and expenses and sometimes integrate with payment systems.

UN Women (2021) notes that digital solutions are becoming part of women's entrepreneurship support programmes globally, as they can improve record-keeping and

market access. In India, this trend is reinforced by government and bank initiatives that promote QR-based payments for small merchants and SHG members.

2.2. **Opportunities and Constraints:** Digital finance offers various potential benefits for women-led enterprises:

- Faster and traceable transactions with customers and suppliers.
- Creation of transaction histories that may support future credit applications.
- Reduced need to carry cash, which can be important where women face risks of theft or intra-household appropriation of earnings.
- Time savings, significant for women balancing paid work and unpaid care responsibilities.

At the same time, several constraints limit uptake and confident use:

- Digital literacy gaps: Many women are first-generation smartphone users, unfamiliar with financial and technical terminology (MicroSave Consulting, 2020).
- Shared device and SIM use: Phones and SIMs may be registered in a male relative's name, and PINs or passwords are often shared, reducing both privacy and security.
- Fear of fraud and irreversibility: Negative experiences—either personal or in the community—create a perception that "if money is lost online, it cannot be recovered."
- Socio-cultural norms: In some households, men supervise or control women's digital and financial decisions, limiting their autonomy (NITI Aayog, 2021).

These factors mean that trust in digital-finance systems and in the legal-regulatory framework is crucial for sustained adoption.

## 3. LEGAL AND REGULATORY FRAMEWORK

3.1. **Information Technology Act, 2000 and Cybersecurity Initiatives:** The Information Technology Act, 2000 (IT Act), as amended, provides the main legal framework for cyber offences and certain aspects of data protection in India. Key provisions relevant to digital finance include:

- Sections 66C and 66D, which criminalise identity theft and cheating by personation using computer resources.

- Section 43A, which imposes liability on body corporates that are negligent in implementing reasonable security practices for sensitive personal data, resulting in wrongful loss or gain.
- Section 72, which penalises unauthorised disclosure of information obtained in the course of exercising powers under the Act.

In parallel, the Ministry of Electronics and Information Technology (MeitY) has developed cybersecurity strategies and initiatives aimed at strengthening national resilience against cyber threats. Recent documents highlight priorities such as secure digital infrastructure, citizen awareness and better coordination among agencies (MeitY, 2023).

While these frameworks are technology-focused and gender-neutral, their implementation has direct implications for women entrepreneurs who rely on digital-finance platforms.

3.2. **RBI Directions on Digital Payments, Security and Customer Protection:** The Reserve Bank of India (RBI) regulates banks and many digital-payment intermediaries. Several directions are particularly relevant:

- The Charter of Customer Rights sets out principles such as fair treatment, transparency, privacy and effective grievance redress for bank customers (RBI, 2020).
- The Master Direction on Prepaid Payment Instruments (PPIs) prescribes security and due-diligence standards for issuers of wallets and similar instruments (RBI, 2021a).
- The Master Directions on Digital Payment Security Controls mandate regulated entities to adopt robust IT-governance, cybersecurity and risk-management measures for digital channels (RBI, 2022).

RBI has also issued frameworks on customer liability in unauthorised electronic transactions, defining circumstances under which customers may have zero liability or limited liability depending on the nature of the breach and the timeliness of reporting. In principle, these provisions apply equally to women entrepreneurs using bank-linked digital channels.

3.3. **Grievance Redress: Integrated Ombudsman Scheme and Consumer Protection:** The Reserve Bank-Integrated Ombudsman Scheme, 2021 consolidates various earlier ombudsman schemes and provides a unified mechanism for resolving customer complaints against regulated entities (RBI, 2021b). Complaints relating to unauthorised

transactions, failure to reverse failed transactions and deficiency in digital-payment services can be escalated to the Ombudsman after initial attempts at resolution with the service provider.

In addition, the Consumer Protection Act, 2019 allows consumers to seek redress for unfair trade practices or deficient services, including potentially against digital-finance providers. However, micro-entrepreneurs often lack the awareness, resources or confidence to use these mechanisms effectively.

3.4. **Policy Perspectives on Digital Finance and Gender:** Global and national-level reports highlight the importance of secure and inclusive digital finance for women's economic empowerment. The Global Findex Database emphasises that trust and effective consumer protection are essential to move beyond mere account ownership to active and meaningful usage (World Bank, 2022). UN Women's reporting on progress under its strategic plan points to digitalisation, including in finance, as both an opportunity and a site of vulnerability for women, particularly in the context of COVID-19 (UN Women, 2021).

In India, policy discussions on the platform economy and gig work similarly underline the need to ensure that digital financial tools are safe and accessible for women workers and entrepreneurs (NITI Aayog, 2021).

## 4. GENDERED CHALLENGES: PRIVACY, CYBERSECURITY AND TRUST

4.1. **Device Sharing, Control and Financial Privacy:** A significant number of women, especially in low-income and rural settings, do not own a personal smartphone. Instead, they rely on shared devices controlled by other family members. Even when the phone is nominally theirs, passwords and PINs may be known to others. This undermines:

- **Informational privacy:** Business income, balances and credit usage are visible to others, affecting women's bargaining power and autonomy.
- **Account security:** Shared or written-down credentials make it easier for insider abuse or accidental disclosure.

These issues are rarely recognised in formal cybersecurity frameworks, yet they are central to women's experience of "security" in digital finance.

4.2. **Cyber Fraud and Barriers to Reporting:** Common frauds affecting digital-finance users include phishing calls, fake UPI links, malicious QR codes and remote-access scams. MicroSave Consulting (2020) notes that women often feel particularly vulnerable

due to limited technical familiarity and fear of being blamed if something goes wrong. Barriers to reporting include:

- Uncertainty about which institution to approach (bank, app-provider, cyber-crime cell, police, or consumer forum).
- Perception that authorities may not take small-value complaints seriously, even though such losses can be large relative to their capital.
- Social stigma or family criticism that may follow public disclosure of having been defrauded.

These barriers mean that many incidents go unreported, reducing both deterrence and the real-world impact of legal protections under the IT Act and RBI guidelines.

4.3. **Data Collection, Profiling and Aggressive Marketing:** Digital-finance apps frequently collect extensive data on users' behaviour, contacts, location and transactions. Without strong data-protection standards and transparent privacy notices, such data can be misused, for example:

- Intensive marketing of credit products to women entrepreneurs who may not fully understand the terms.
- Algorithmic profiling that classifies users as "high risk" based on opaque criteria, potentially affecting access to services.
- In extreme cases, abusive recovery practices that use personal contacts or images in ways that amount to harassment.

While the legal landscape on data protection in India is evolving, effective enforcement and user comprehension remain major challenges.

4.4. **Trust Deficits and the Gap Between Law and Practice:** Although the legal and regulatory framework on paper appears reasonably comprehensive, trust deficits persist. Studies indicate that women's usage of digital financial services is often cautious and limited, even when they have access (MicroSave Consulting, 2020; World Bank, 2022). Reasons include:

- Low awareness of RBI's customer-protection framework, zero-liability provisions or Ombudsman mechanisms.
- Complex and time-consuming complaint procedures.
- Previous experiences of unresolved issues or poor service.

As a result, women may revert to cash or use digital channels only when unavoidable. This gap between de jure rights and de facto experience is central to understanding why legal protections alone are not sufficient.

## 5. TOWARDS GENDER-RESPONSIVE LEGAL AND POLICY RESPONSES

5.1. **Strengthening Legal and Digital Literacy**: Targeted legal and digital-literacy programmes for women entrepreneurs are essential. Building on insights from MicroSave Consulting (2020) and UN Women (2021), such programmes should:

- Explain common digital-fraud tactics and safe-usage practices.
- Inform women of their rights under RBI's customer-protection framework and Ombudsman Scheme.
- Provide step-by-step guidance on how to file complaints and follow them up.

These efforts can be integrated into SHG federations, entrepreneurship-development programmes, and bank outreach activities, and must be offered in local languages.

5.2. **Simplifying and Localising Grievance-Redress Mechanisms**: To make redress genuinely accessible:

- Local facilitation desks at bank branches, common service centres or SHG offices can assist women in drafting and submitting complaints.
- Digital-payment apps can embed simple complaint-buttons with guided flows in local languages.
- Awareness campaigns can publicise the existence and scope of the Integrated Ombudsman Scheme (RBI, 2021b).

The goal is to reduce procedural complexity so that women can realistically seek remedies when their rights are violated.

5.3. **Gender-Sensitive Design and Privacy-by-Default:** Service providers and regulators should encourage user-centric design features that respond to women's privacy needs, such as:

- Interfaces in multiple Indian languages with clear, non-technical explanations.
- Options to hide sensitive information (e.g., balances, loan details) from lock-screen notifications.
- Clear, granular consent requests that allow users to refuse non-essential data sharing.

Such “privacy-by-default” and “safety-by-design” measures can significantly improve women’s confidence in digital-finance tools.

5.4. **Strengthening Data-Protection and Security Governance**: In this context, as India’s broader data-protection and cybersecurity frameworks are developed, financial data should be treated as particularly sensitive. Regulatory priorities might include:

- Stronger obligations on fintechs and payment intermediaries regarding data minimisation, purpose limitation and breach notification.
- Regular independent security audits, with summary findings shared with regulators.
- Clear liability rules and penalties for negligent handling or misuse of customer data.

These measures would align with global best practices emphasised in international policy discussions (World Bank, 2022; UN Women, 2021).

Framing financial-data protection and cybersecurity as enablers of SDG 5, SDG 8 and SDG 16 can help align regulatory action with India’s international commitments and provide a clearer basis for monitoring progress in women’s digital-financial inclusion.

## 6. CONCLUSION

Digital finance is central to contemporary financial-inclusion strategies in India and is increasingly woven into programmes aimed at supporting women’s entrepreneurship. For women-led micro and small enterprises, digital tools can reduce transaction costs, create financial histories and potentially strengthen economic autonomy.

However, as this paper has argued, the benefits of digital finance for women entrepreneurs are not guaranteed. Despite the existence of a formal legal and regulatory framework—covering cyber offences, payment security, customer protection and emerging cybersecurity strategies—women face distinct challenges. Shared device usage, low digital and legal literacy, socio-cultural constraints and complex redress procedures all affect their exposure to risks and their willingness to trust digital-finance systems.

From a socio-legal perspective, trust is as important as technical security. Building this trust requires not only stronger rules, but also gender-responsive implementation: targeted literacy efforts, simplified and localised grievance-redress mechanisms, user-centric design of digital-finance tools and rigorous enforcement of data-protection and security standards.

If these elements can be integrated effectively, digital finance has the potential to contribute meaningfully to women's entrepreneurial empowerment and inclusive growth in India, in line with the country's commitments under the Sustainable Development Goals, particularly SDG 5 on gender equality, SDG 8 on decent work and economic growth, and SDG 16 on strong, inclusive institutions (United Nations, 2015).

## REFERENCES


1. MicroSave Consulting. (2020). Why are women in India not using digital financial services as much as men? MicroSave Consulting. https://www.microsave.net
2. Ministry of Electronics and Information Technology. (2023). Cyber security [Webpage and policy documents]. Government of India. https://www.meity.gov.in/cyber-security
3. NITI Aayog. (2021). India's booming gig and platform economy: Perspectives and recommendations on the future of work. Government of India. https://www.niti.gov.in
4. Reserve Bank of India. (2020). Charter of customer rights. Reserve Bank of India. https://www.rbi.org.in/commonman/English/Scripts/Notification.aspx?Id=11246
5. Reserve Bank of India. (2021a). Master direction on prepaid payment instruments (PPIs). Reserve Bank of India. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12103&Mode=0
6. Reserve Bank of India. (2021b). Master direction – Reserve Bank-Integrated Ombudsman Scheme, 2021. Reserve Bank of India. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12193&Mode=0
7. Reserve Bank of India. (2022). Master directions on digital payment security controls. Reserve Bank of India. https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12211&Mode=0
8. United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development* (A/RES/70/1). United Nations. https://sdgs.un.org/2030agenda
9. UN Women. (2021). Report of the Under-Secretary-General/Executive Director of the United Nations Entity for Gender Equality and the Empowerment of Women on progress made on the Strategic Plan 2018–2021 (UNW/2021/2). United Nations Entity for Gender Equality and the Empowerment of Women.
10. World Bank. (2022). The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19. World Bank. https://www.worldbank.org/en/publication/globalfindex