European Economic Letters
ISSN 2323-5233
Vol 15, Issue 2 (2025)
http://eelet.org.uk

Legislative Trends: Strengthening E-Rupee against Financial Cybercrime through a Human-Centric Approach

Kiran Pal Singh[1*], Dr. (Prof.) Jogiram Sharma[2]
[1*] Ph.D. Research Scholar, Dept. of Law, Geeta Global Law School,
Geeta University, Panipat, Haryana-132145,
[2] Guide cum Director, Dept. of Law, Geeta Global Law School,
Geeta University, Panipat, Haryana-132145,

Abstract:

India's push toward a Central Bank Digital Currency (CBDC), the e-Rupee, in 2024 has been accompanied by significant legislative and regulatory developments aimed at fortifying digital payment systems against cybercrime, fraud, and identity misuse. This paper surveys these developments through a human-centric lens, focusing on how new laws and amendments enhance user protection, data privacy, and the integrity of the digital financial ecosystem. Key trends include amendments to the Reserve Bank of India Act recognizing the e-Rupee as legal tender and empowering the Reserve Bank of India (RBI) to pilot a secure CBDC framework; proposed overhauls of the Information Technology Act, 2000 via a forthcoming Digital India Act to address modern cyber offences; the enactment of the Digital Personal Data Protection Act, 2023 to safeguard personal data and prevent identity theft; and updates to criminal laws (Bharatiya Nyaya Sanhita, 2023) explicitly penalizing cyber fraud and identity-related crimes. The paper provides a descriptive legal analysis of these measures – interpreting key provisions, examining their constitutional validity and enforcement, identifying remaining loopholes, and critiquing policy choices. Indian efforts are contextualized with international frameworks, including the EU's proposed digital euro legislation, robust data protection regimes, and global cybercrime cooperation conventions. Figures and tables illustrate legislative timelines, cybercrime statistics, and comparative regulatory models. The analysis concludes that India's 2024 legislative trajectory reflects a proactive but evolving approach, blending technological innovation with legal safeguards to foster trust in the e-Rupee and resilience against financial cybercrime.

Keywords: E-Rupee; Legislative Reforms, Financial Cybercrime; Digital Personal Data Protection; CBDC;

1. Introduction

Digital payments in India have witnessed explosive growth over the past decade, bringing convenience alongside new vectors for fraud and cybercrime. The e-Rupee, India's nascent Central Bank Digital Currency (CBDC) launched in pilot form by the RBI, epitomizes this digital financial revolution [1]. As India embraces the e-Rupee, lawmakers and regulators in 2024 have grappled with the challenge of strengthening legal frameworks to safeguard users (a human-centric focus) and preserve trust in digital money. High-profile cyber frauds, identity theft cases, and misuse of personal data have underscored the need for robust legislation that balances innovation with security and privacy [2]. Crucially, 2024 saw a confluence of legislative initiatives at both central and state levels targeting the twin pillars of a secure e-Rupee ecosystem: financial regulation (to enable and protect the CBDC and digital payments) and cybersecurity law (to deter and punish cybercrimes and data misuse). Central statutes like the Reserve Bank of India Act, the Information Technology Act, and the new Digital Personal Data Protection Act were at the forefront, with important amendments and rules coming into force. Simultaneously, India undertook criminal law reforms by replacing the colonial-era Indian Penal Code with the Bharatiya Nyaya Sanhita, 2023, which introduces specific offences for cyber fraud and identity crimes [3]. These developments signal an evolving legal landscape geared toward a human-centric approach – prioritizing consumer protection, privacy rights, and accessible justice – in the face of sophisticated financial cyber threats.

This review paper examines these legislative trends in detail, focusing on changes during 2024. It analyzes how new laws and regulations strengthen the e-Rupee framework and mitigate risks of cyber fraud and identity misuse. The analysis covers enacted laws and proposed bills, government notifications, and regulatory guidelines, including amendments to the RBI Act that legally empower the digital rupee, enhancements to cybercrime provisions via the IT Act (and its anticipated successor, the Digital India Act), the implementation of the Digital Personal Data Protection Act, and other relevant financial regulations such as anti-money laundering measures. The constitutional validity and practicality of these measures are critically evaluated, identifying areas where legal loopholes or enforcement gaps persist. To broaden perspective, the paper compares India's efforts with select international legal frameworks governing CBDCs and cybersecurity – for instance, the European Union's digital euro initiative and global cybercrime cooperation norms – highlighting best practices and gaps in India's approach. By situating India's 2024 legislative developments in a comparative context and emphasizing a human-

centric lens, the paper provides insight into how law and policy are responding to the emerging threats in digital finance. The goal is to inform a legislative trends discourse on whether India's current trajectory can effectively bolster the e-Rupee's resilience against cybercrime while upholding citizens' rights and trust in the digital economy.

2. The E-Rupee (Digital Rupee) and Its Legal Foundations:

Figure 1: Official logo and tagline of the Digital Rupee (e₹) issued by RBI (emphasizing it is "Cash, but Digital!")

India's Digital Rupee (e₹) – the RBI-issued CBDC – was conceptualized to complement physical currency with a digital legal tender. Legally, the foundation for the e-Rupee was laid by amendments to the Reserve Bank of India Act, 1934. Through the Finance Act, 2022, Parliament modified the RBI Act to include digital currency: the definition of "bank note" now expressly encompasses "whether in physical or digital form" [4]. This pivotal change gave the RBI clear authority to issue digital legal tender. Section 26 of the RBI Act (as amended) thus affirms that e-Rupee is legal tender in India, on par with paper currency. By according the e-Rupee the status of sovereign currency, backed by the guarantee of the central government and liability of RBI, the amendment ensured that transactions in e-Rupee carry the same finality and trust as cash [5].

Regulatory framework: Following the RBI Act amendment, the RBI rolled out pilots for the e-Rupee in late 2022 and 2023. While no separate "Digital Rupee Act" was enacted, the RBI has used its existing powers under the RBI Act and Payment and Settlement Systems Act, 2007 to regulate the issuance and distribution of the e-Rupee. For instance, RBI issued a Concept Note (2022) and engaged the RBI Innovation Hub to develop the CBDC. In 2024, the RBI expanded pilot programs to test e-Rupee's functionality (including offline transactions) and interoperability with existing payment platforms. These pilots are accompanied by RBI directions to participant banks on technology and security standards, ensuring a secure implementation. Notably, in February 2024 the RBI announced trials of an offline e-Rupee to enable transactions in low-connectivity areas, reflecting a policy thrust to mirror cash-like resilience in digital form [6].

Cybersecurity provisions: A critical aspect of strengthening the e-Rupee system is protecting it against cyber vulnerabilities. The RBI has emphasized that robust cybersecurity frameworks must undergird the CBDC infrastructure [7]. Although the e-Rupee itself is issued by RBI, the wallets and apps facilitating its retail use are offered by banks and regulated entities [8]. These intermediaries must comply with stringent IT security norms. In late 2023, the RBI issued comprehensive Master Directions on IT Governance and Cybersecurity for banks and NBFCs, which took effect from April 1, 2024. These directions consolidate earlier guidelines and impose board-level responsibility on financial institutions to safeguard customer data and digital transactions. They define "cyber incidents" broadly and mandate continuous monitoring, incident reporting, and cyber-resilience measures for all digital banking products. Such regulatory steps directly benefit the e-Rupee ecosystem by hardening defenses against hacking, fraud, and operational disruptions [9].

Interpretation and validity: The RBI Act amendments for digital currency have not faced serious constitutional challenge – issuance of currency lies within the Union's legislative domain (Entry 36, List I, Seventh Schedule of the Constitution). By using a Finance Act amendment, the change was procedurally in order, and it aligns with public policy to modernize currency. One notable aspect is privacy: as a sovereign digital currency, the e-Rupee raises concerns about potential state surveillance of transactions. While not explicitly addressed in legislation, RBI officials have indicated an intention to incorporate privacy features akin to cash (e.g., anonymity for small transactions) in the CBDC design [10]. Balancing traceability (for crime prevention) with user privacy is an ongoing policy challenge. A human-centric legal approach would require transparent data governance rules for the e-Rupee – possibly via RBI regulation or under the data protection law (discussed later) – to ensure that users' transactional privacy is respected in the absence of specific statute on CBDC privacy.

Implementation challenges: As of 2024, the e-Rupee is in pilot stage, with about 1.5 million users and 0.4 million merchants enrolled in pilots [11]. The legal framework seems adequate for this phase; however, full-scale implementation may demand additional legislation or rules. For example, fraud liability in e-Rupee transactions (who bears loss if a wallet is hacked) is not yet delineated in law and likely defaults to existing banking ombudsman norms. Clear rules on this and on grievance redress mechanisms specific to CBDC will be important. Another gap is the still-pending Cryptocurrency and Official Digital Currency Bill (first proposed in 2021) which aimed to ban or regulate private cryptocurrencies while facilitating CBDC. That bill has not been enacted as of 2024; instead, India adopted an interim approach of taxation and

RBI oversight for crypto. The absence of a comprehensive crypto law means that the e-Rupee operates in a landscape where private digital assets are partly regulated (through tax and anti-money laundering laws) but not outlawed. Some commentators argue that a clearer legal distinction between the state-backed e-Rupee and other virtual assets is needed to prevent confusion and illicit arbitrage [12]. In summary, the legal groundwork for the e-Rupee – principally via RBI Act amendments and RBI regulations – is largely in place and constitutionally sound. The focus has now shifted to strengthening operational security and building user trust through regulatory oversight. As the subsequent sections show, parallel legislative measures in 2024 dealing with cybercrime, data protection, and financial regulation all contribute to creating an environment in which the e-Rupee can flourish safely and securely.

3. Legislative Trends in India: A 2024 Overview

3.1. Bolstering Cybercrime Laws: IT Act, Proposed Digital India Act, and Criminal Law Reforms:

The proliferation of digital transactions (from UPI to e-Rupee) has rendered India's cybercrime laws more critical than ever. The primary law addressing cyber offences, the Information Technology Act, 2000 (IT Act), though path-breaking when enacted, has seen limited updates since the 2008 amendments. By 2024, the government acknowledged that the IT Act requires an overhaul to tackle contemporary challenges such as digital impersonation scams, online fraud, and new technologies (e.g. AI-based cybercrimes). Accordingly, a Digital India Act has been in the drafting stage to replace the IT Act. While the Digital India Act was not finalized in 2024, the Ministry of Electronics and IT (MeitY) undertook consultations and indicated key directions of the proposed law, even as certain interim tweaks to existing rules were made.

Status of IT Act in 2024: The IT Act currently criminalizes various cyber offences: e.g., Section 66C (identity theft, punishment up to 3 years imprisonment), Section 66D (cheating by personation using computer, up to 3 years), Section 66E (violation of privacy by publishing private images, etc.), Section 67B (child pornography), and Section 66F (cyber terrorism, up to life imprisonment). These provisions, read with Indian Penal Code sections (for cheating, extortion, etc.), form the basis of prosecuting cybercriminals. However, notable gaps have been identified. For instance, phishing and online fraud often involve impersonation, which is covered, but the investigative procedures and jurisdiction issues (crimes spanning states or countries) strain existing frameworks. Additionally, the infamous Section 66A (which penalized "offensive" online messages) was struck down by the Supreme Court in Shreya Singhal v. Union of India (2015) on free speech grounds, highlighting the need for careful calibration of cyber laws with constitutional rights. Since then, no comprehensive amendment has addressed new forms of cyber harm like deepfakes, cyberstalking in detail, or frauds exploiting emerging platforms – issues presumably to be taken up by the Digital India Act.

Proposed Digital India Act: Although a draft Bill was not publicly released in 2024, statements from officials suggest its scope. The Act is expected to be a "next-generation" IT law covering not just conventional cyber offences but also systemic regulation of the internet ecosystem (intermediaries, AI, data, etc.). MeitY officials have indicated the new law may categorize intermediaries (e.g., social media, e-commerce, payment platforms) and assign graded obligations, ideally through legislation rather than just executive rules. There is recognition that issues like deepfakes (mentioned as high-quality misrepresentations) can be tackled under existing law for fraud or impersonation, but more explicit provisions and faster takedown mechanisms may be needed. Importantly, MeitY's stance as of end-2024 was not to rush the Digital India Act, given that "the existing legal framework…is satisfactory at the moment" in handling current risks. The ministry expressed openness to incremental amendments to the IT Act if urgent issues arise, rather than introducing an all-new bill without consensus. This cautious approach suggests that the Digital India Act, when it comes, will be thoroughly deliberated – a positive from a constitutional perspective, ensuring new provisions (for instance, on content moderation or encryption) are vetted for consistency with fundamental rights [13].

2024 interim measures: In absence of the new Act, the government relied on subordinate legislation under the IT Act to address pressing issues. Notably, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules were amended in 2023 to deal with fake online content and online games. One amendment (April 2023) sought to have a government-notified "fact-check unit" flag false information related to the government, mandating intermediaries to take it down – a move criticized as enabling censorship and currently under legal challenge. While not directly related to financial cybercrime, this shows the government's tendency to use rules to fill gaps pending a new Act. Another domain is critical information infrastructure and cyber incident reporting: the Indian Computer Emergency Response Team (CERT-In) in 2022 (operating under Section 70B of IT Act) issued directions making it mandatory for companies (including financial entities) to report cybersecurity incidents within hours and maintain server logs [14][15]. In 2023-24, compliance with these directions has improved detection and response to cyberattacks, indirectly protecting financial systems (e.g., quick containment of malware outbreaks affecting payment systems) – though some industry players raised privacy concerns over data retention requirements.

On the criminal justice front, a landmark development was the passage of the Bharatiya Nyaya Sanhita (BNS) 2023, which will replace the IPC once brought into force (likely from 2024). The BNS introduces explicit provisions for cybercrime. For example, it emphasizes digital offences by naming cyber fraud, identity theft, and digital harassment as specific crimes requiring attention [16]. Traditional offences are redefined to account for digital property and instruments – theft now clearly encompasses theft of digital data as "movable property" and misappropriation or siphoning of digital assets falls under criminal misappropriation [17]. Organized cybercrimes conducted by syndicates are addressed by treating them as organized crime with enhanced penalties. The BNS's focus on modernizing language and scope of crimes is evident: it aims to remove ambiguity that existed under IPC when dealing with intangibles. By explicitly listing cyber fraud and identity theft, the law gives confidence that acts like phishing scams, SIM swap frauds, or illegal use of someone's digital identity will be prosecutable with clarity. The BNS also reflects a victim-centric approach and faster procedures, which could benefit victims of financial cybercrime through faster trials or summary restitution orders [18]. Indeed, some states have innovated on restitution – Gujarat and Karnataka, for instance, use Lok Adalats or magistrates to swiftly return defrauded money to victims' accounts when the beneficiary is identifiable. Integrating such practices within the formal law (e.g., empowering courts to freeze and reverse e-transactions in fraud cases) could be a next step [19].

Enforcement and capacity: Strengthening laws is only one side of the coin; enforcement capacity is equally vital. In 2024, the Indian Cyber Crime Coordination Centre (I4C) under MHA reported alarming statistics: over 1.5 million cybercrime complaints were made in 2023 (a 61% jump from 2022) and over 740,000 in just the first four months of 2024. About 85% of these related to financial fraud, such as UPI scams, card frauds, and loan app scams – directly impacting digital financial security [20]. This surge (illustrated in Figure 2 below) has pressured law enforcement agencies to adapt. The government in 2024 continued to expand dedicated cyber police stations, training for officers in cyber forensics, and public awareness campaigns (including the 24x7 national helpline '1930' for rapid fraud reporting). The citizen reporting portal and helpline have enabled freezing about ₹1,127 crore of defrauded money before it left the system (about 9–10% of losses)– a notable recovery rate that showcases an increasingly human-centric enforcement approach, focusing on minimizing harm to victims [21].

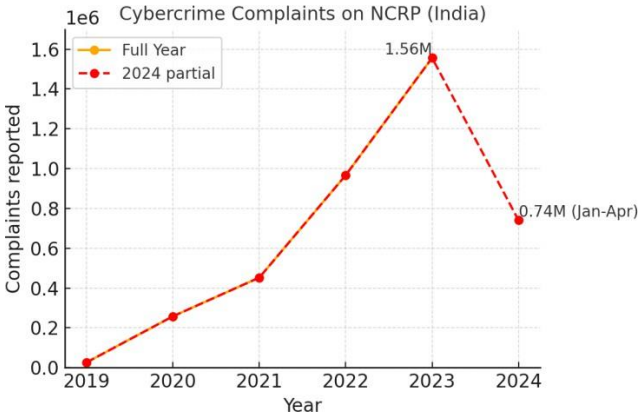

Figure 2: Rising cybercrime complaints in India, 2019–2024 (data from National Cybercrime Reporting Portal). Financial frauds constitute the majority of these complaints.

Despite these efforts, challenges remain: cross-border cybercrimes (nearly half of complaints involve perpetrators from abroad, e.g., Southeast Asia) require international cooperation which is still nascent (India is not yet a party to the Budapest Convention on Cybercrime). Additionally, the backlog in courts means that conviction rates for cyber offences are low relative to incidence – a gap that legal reforms like specialized cyber courts or fast-track procedures in the new laws might need to address. In sum, 2024's legislative trend in cybercrime law reflects incremental strengthening. The existing IT Act framework, though strained, was patched via rules and is buttressed by the new Data Protection Act and criminal code updates. The forthcoming Digital India Act represents a crucial opportunity to craft a holistic legal architecture for the digital realm, one that can more comprehensively tackle cyber offences related to e-finance. Meanwhile, the Bharatiya Nyaya Sanhita's recognition of cyber offences and the continued push for better enforcement mechanisms point toward a legal system gearing up to support the safe usage of e-Rupee and other digital services through stronger deterrence and user-centric remedies [22].

3.2. Data Protection and Identity Security: The Digital Personal Data Protection Act, 2023:

Protecting personal and financial data is central to a human-centric strategy against cybercrime. One of the most significant legislative developments affecting the digital ecosystem in 2023–24 was the enactment of the Digital Personal Data Protection Act, 2023 (DPDP Act). Passed by Parliament in August 2023, the DPDP Act came into force in parts toward late 2023, with full enforcement expected in 2024. It establishes India's first comprehensive regime for personal data protection and replaces the patchwork of rules under the IT Act (notably, it repeals Section 43A of the IT Act, which had provided a limited data protection obligation on companies) [23]. The Act's impact on financial cybercrime and identity misuse is indirect but critical: by imposing duties on entities to secure personal data and prevent its misuse, the law aims to reduce

data breaches, identity theft, and fraud that exploit leaked data [24].

Key Features Relevant to Financial Data: The DPDP Act governs digital personal data—any identifiable individual's information in digital form. This includes financial data such as bank account details, Aadhaar, PAN, UPI IDs, biometric KYC data, and transaction history. Financial firms and fintech companies qualify as "Data Fiduciaries" and must adopt appropriate safeguards to prevent data breaches (Section 8). In case of a breach, they are obligated to notify the Data Protection Board and potentially the affected individuals. Strict penalties, up to ₹250 crore, incentivize stronger cybersecurity practices. Though the Act doesn't categorize "sensitive" data, the government can label certain data types as "high risk" and impose extra protections.

Individual Rights:
The law grants users (Data Principals) rights such as access to their data and the ability to correct or delete it. While it lacks strong data portability or erasure rights, individuals may still request deletion after discontinuing a service, reducing exposure to breaches. A user can also authorize someone to exercise their rights posthumously.

Government Access and Exemptions:
The central government may exempt specific agencies from compliance for reasons like national security or public order. Though globally common, such exemptions raise privacy concerns if not applied proportionately, potentially challenging constitutional privacy rights.

Compensation and remedies: One notable omission in the DPDP Act is the ability for individuals to claim compensation for data misuse. In the earlier regime (IT Act Section 43A and tort law), an individual could sue for damages if a company's negligence caused a data leak. The DPDP Act, however, replaces that with a model of regulatory fines. Section 43A and 72A (which gave a cause of action for breach of confidentiality) are repealed [25]. This means a victim of identity theft due to a bank's lax security cannot directly claim damages from the bank under this Act; they must rely on the Data Protection Board to impose fines on the bank (which go to the state, not the victim). As observers noted, by repealing the compensation provision without replacement, the Act "deprives vulnerable groups of existing remedies", leaving them only the option to complain to the Data Protection Board. This has been critiqued as a step back in ensuring full restitution for harm. A human-centric law might have included an easy mechanism for individuals to be compensated for losses (for example, identity theft leading to monetary loss). This gap might be filled by consumer protection laws or sectoral regulations in the interim (for example, RBI could mandate banks to compensate customers for certain unauthorized digital transactions, as it does under its limited liability for card fraud framework).

Interface with financial sector laws: The DPDP Act's requirements dovetail with other regulatory initiatives. For instance, RBI's guidelines on digital payment security (the Digital Payment Security Controls, 2021 [26] already mandated banks to implement strong authentication (like device binding, biometric authentication) to protect user accounts. The DPDP Act adds legal force by making protection of the underlying personal data (device IDs, biometrics) a compliance issue not just a security best practice. Similarly, SEBI and IRDAI (for securities and insurance sectors) have their own cyber resilience guidelines; they will all operate in concord with the DPDP Act's umbrella framework. Over time, one can expect harmonization – e.g., a breach reported to the Data Protection Board will likely also be reported to sectoral regulators to coordinate responses [27].
Constitutional validity: The DPDP Act is an outcome of the Supreme Court's declaration of privacy as a fundamental right, which urged the government to pass a data protection law. In that sense, it furthers constitutional goals. However, certain provisions could be flashpoints for constitutional litigation. Broad executive powers (like notifications to exempt government agencies or to compel businesses to furnish personal data in "public interest") might be tested for proportionality. Additionally, the Data Protection Board's independence is questionable – it is constituted by the government, raising concerns about regulatory autonomy in adjudicating violations by government entities themselves. If the Board is seen as not independent, that could undermine effective remedy and thus be challenged as illusory enforcement. These issues have been debated in civil society, but as of 2024 no court case has arisen yet (the Act is too new). It will be important that rules made under the Act (which were under consultation in late 2024address transparency and due process to reinforce the Act's constitutionality.
Implementation outlook: The effective implementation of the Digital Personal Data Protection (DPDP) Act is critical to combating identity-based cybercrimes in India. In 2024, the government began establishing the Data Protection Board and releasing draft rules to guide enforcement. One major challenge is raising public awareness—citizens must understand their data rights, such as the ability to refuse consent for unnecessary data collection. This knowledge can help reduce phishing attacks, many of which exploit individuals' lack of awareness through tactics like tricking users into sharing OTPs or sensitive personal information. Organizations are beginning to roll out compliance programs, including upgrading their IT

infrastructure to improve data encryption and implement systems for managing consent. A transitional period may follow, where data breaches still occur—as seen in 2023 with several leaks in both fintech and government sectors. However, the Act's steep penalties, reaching up to ₹250 crore (about USD 30 million), are expected to drive stronger cybersecurity measures over time. The Act also indirectly strengthens protections around digital identity systems such as Aadhaar. While Aadhaar is governed separately, the DPDP Act applies to its use by private entities, ensuring such data is handled securely and only with consent. Ultimately, the DPDP Act promotes a human-centric digital ecosystem by prioritizing individual autonomy and building trust in systems like e-Rupee.

4. Financial Regulatory Measures and Notifications in 2024:

Beyond primary legislation, secondary regulations and government notifications in 2023–24 have played an important role in shoring up the defenses of India's digital finance system against cybercrime and illicit use. These measures often derive their authority from existing laws but represent nimble responses by regulatory bodies to emerging threats. We highlight a few notable developments:

1. Anti-Money Laundering (AML) expansion to Virtual Assets: In a significant step, the Ministry of Finance issued a notification on 7 March 2023 bringing virtual digital assets (cryptocurrencies) and related service providers under the ambit of the Prevention of Money Laundering Act, 2002 (PMLA). This means cryptocurrency exchanges, custodians, and wallet providers must follow KYC norms, record-keeping, and report suspicious transactions to the Financial Intelligence Unit (FIU). While this move was not about the e-Rupee per se, it complements India's approach of differentiating legitimate digital currency from private crypto. By tightening oversight of crypto transactions (often used in fraud or ransomware payments), the government aimed to reduce financial crime risk as the e-Rupee was rolled out. The AML notification effectively signals that any digital value transfer – be it crypto or e-Rupee – is subject to scrutiny and traceability to deter misuse. It also aligns India with FATF recommendations on virtual assets, improving international cooperation against money laundering and terror financing in the cyber realm [28].

2. Know Your Customer (KYC) and identity verification norms: The RBI and SEBI in 2023 issued updated KYC guidelines to further ease and secure the customer onboarding process in digital platforms. For example, RBI's Master Direction on KYC (updated May 2023) enabled Video KYC and Aadhaar-based e-KYC as standard, while also mandating periodic KYC updates and tighter KYC for high-risk accounts. This regulatory trend walks a fine line: making digital onboarding seamless (to encourage fintech innovation and inclusion) yet ensuring robust verification to prevent fake identities. Better KYC directly mitigates identity fraud – many loan app scams and mule accounts in payment frauds involve identity theft or synthetic identities. Under stricter KYC norms, banks are now required to cross-check customer identity across the Central KYC Registry and report anomalies. Additionally, the UIDAI (Aadhaar authority) mandated masked Aadhaar and secure QR codes to verify identities without exposing full Aadhaar numbers, thereby reducing chances of misuse of ID data. These efforts are not "legislation" per se, but regulatory rules under existing laws (RBI Act, Aadhaar Act, etc.), and they contribute to plugging loopholes that cybercriminals exploited in the past.

3. Payment fraud safeguards: The RBI has also used its powers under the Payment and Settlement Systems Act, 2007 to issue directions aimed at consumer protection in digital payments. A notable measure is the Limited Liability Circular (2017, reaffirmed in 2019) which sets rules for customer liability in unauthorized electronic banking transactions. Under this, if a customer reports an unauthorized transaction (say, due to phishing) within 3 days, their liability is zero; the bank eats the loss. This has indirectly forced banks to strengthen real-time fraud monitoring and customer education (to avoid such incidents). In 2024, RBI continued to stress compliance with this framework and published data on banks' handling of fraud claims. The enforcement of this rule is a human-centric approach, ensuring victims of cyber fraud are not financially devastated (provided they act promptly). Moreover, NPCI (which operates UPI) introduced features like UPI fraud reporting via the app and 24-hour reversal mechanisms for reported frauds, working within the NPCI's regulatory supervision by RBI. These measures, though granular, reflect the closing of implementation gaps – turning laws on paper into actual relief for users.

4. State-level initiatives: While states in India cannot legislate on banking or currency (Union subjects), they play a role in law enforcement and certain areas like policing identity systems. Some state governments in 2024 launched special cybersecurity policies or set up task forces. For instance, Telangana came up with a Cyber Security Framework for its government IT systems, and Maharashtra strengthened its Cyber Police department with advanced training – these executive actions contribute to overall resilience. On the legislative side, a few states tackled related issues: e.g., various states passed or considered laws to regulate online gambling and betting apps (Tamil Nadu's Online Gaming Prohibition Act, 2022 was an example). Although targeted at gambling, such laws also have an effect on curbing illicit online financial flows and

associated fraud (many fraudulent apps masquerade as gaming or investment platforms). Another example at state level is the use of Aadhaar verification for certain services – some states require Aadhaar authentication for high-value property transactions to curb benami deals and fraud, indirectly bolstering identity verification in financial dealings. These efforts complement national legislation by addressing local modus operandi of cybercriminals.

5. "Vishwasya" Blockchain infrastructure (2024): In August 2024, the Ministry of Electronics & IT launched the Vishvasya Blockchain Technology Stack, a national project to provide a reliable blockchain infrastructure for applications. While not a law, this initiative (whose Sanskrit name "Vishvasya" means trustworthy) aims to create indigenous blockchain platforms for uses like credential storage, supply chains, and possibly digital currencies. A robust, auditable blockchain run by the government could enhance the security of e-Rupee transactions (if leveraged by RBI for certain backend functions) and reduce dependence on foreign tech. It exemplifies a technological response in parallel with legal responses – recognizing that technology design (ensuring transparency, immutability) can reduce certain fraud opportunities (like double-spending or unauthorized ledger changes in a CBDC system). Legal policy encourages such innovation: the government's Digital India initiatives often dovetail tech deployment with necessary legal underpinnings (for instance, using electronic ledgers as evidence is facilitated by amendments in evidence law, etc.) [29].

Policy critique: While these financial regulatory measures are certainly steps forward, policy analysts have noted some gaps. The AML extension to crypto is effective, but India still lacks a dedicated Cryptocurrency Regulation law – leaving ambiguity over the legal status of crypto holdings (aside from taxation). This could become problematic if, for example, a fraudster holds proceeds in crypto; enforcement agencies have tools to trace and freeze via AML, but prosecution under a clear prohibitory law is missing. Similarly, KYC norms tightening is good, but over-reliance on Aadhaar has its own risks (if Aadhaar itself is compromised or if biometric authentication is spoofed). A diversified multi-factor identification regime may be more resilient. The RBI and government could consider mandating multi-factor auth for all high-value transactions (some of which is already in place via OTP/PIN, but perhaps additional device or biometric checks for critical transfers). Finally, international cooperation measures could be strengthened. In 2024, India was actively participating in drafting a proposed UN Cybercrime Convention and had engaged with INTERPOL on cybercrime operations. However, India has held off joining the Budapest Convention, citing sovereignty concerns. As cross-border frauds rise, aligning domestic laws with global frameworks (while safeguarding sovereignty) will be crucial. This might entail legislative changes in coming years to allow streamlined evidence sharing, extradition for cyber offences, etc. – building on the foundation laid in 2024.

5. Comparative Perspectives: International Laws on Digital Currency and Cybersecurity:

India's approach in 2024 to legislating for digital currency security and cybercrime can be better understood in light of international developments. Many jurisdictions are grappling with similar issues – how to regulate emerging digital payment forms (including CBDCs) and how to update cyber laws for the modern age. Here we compare select aspects:
Digital Currency (CBDC) Legal Frameworks: Several countries/regions have moved towards recognizing CBDCs in law. Notably, the European Union in June 2023 proposed a Digital Euro legislative package, aiming to establish the legal tender status of a potential Euro CBDC [30]. The EU proposal, like India's RBI Act amendment, ensures that digital currency issued by the central bank would be universally accepted and has debt-clearing power. It also contains provisions for privacy safeguards, reflecting EU's strong data protection ethos. The proposal needs approval from the European Parliament and Council, and is under debate through 2024.

China took an assertive route by amending its central bank law drafts to recognize the e-CNY (digital yuan) as legal tender and simultaneously banning cryptocurrency trading by a PBOC circular in 2021. China's approach is more centralized: the e-CNY has been rolled out in major cities with a legal framework that tightly controls digital currency use and criminalizes unauthorized digital token issuance [31][32]. Nigeria and some Caribbean nations (like Bahamas with the Sand Dollar) have also introduced CBDCs; Nigeria's eNaira is backed by existing central bank regulations and a cashless policy, though its uptake has been modest.

In comparison, India's approach could be seen as balanced – it gave the CBDC legal backing but did not outlaw crypto through legislation (choosing a wait-and-watch approach combined with taxation/AML measures). This might be contrasted with the United States, where as of 2024 there is no digital dollar and legal changes are only being discussed. The U.S. Federal Reserve has indicated that launching a CBDC would likely require Congressional authorization. Indeed, bills like the proposed "Digital Dollar Pilot Prevention Act" have been introduced to ensure executive agencies don't unilaterally create a CBDC without legislative nod. The U.S. also differs in its handling of crypto: rather than ban, it uses financial regulations (SEC actions, state money transmitter laws) to curb abuses, albeit without a single comprehensive law yet.

Cybersecurity and Data Protection Regimes: India's Digital Personal Data Protection (DPDP) Act draws parallels with the European Union's General Data Protection Regulation (GDPR), which is widely recognized as the global benchmark. While GDPR is stringent, with extraterritorial applicability and substantial penalties, India's approach is more accommodating to business operations. For example, the Indian law does not impose strict purpose limitations on government data use and lacks an independent data protection authority, opting instead for a government-controlled board.
In cybersecurity, the EU's Network and Information Security Directive 2 (NIS2), effective around 2024, sets mandatory security and reporting standards for various sectors. India has sector-specific norms like the RBI's 2023 Master Directions, though these are not uniformly applied across all industries. Data breach reporting under GDPR mandates notification within 72 hours; the DPDP Act is expected to adopt a similar requirement, marking a shift from India's past inconsistencies in reporting breaches.

On cybercrime, while over 65 countries have adopted the Budapest Convention, India has not joined and is pushing for a new UN-led treaty. Countries like Japan, Singapore, and Australia have updated laws to include offenses like cyber espionage and have raised penalties. Singapore's Cybersecurity Act (2018) regulates critical infrastructure, a priority also reflected in India's IT Act and potentially its upcoming Digital India Act. India's Bharatiya Nyaya Sanhita (BNS) 2023 reflects global trends of updating colonial-era laws, much like Japan and the UK have done.
Globally, a people-centric digital legal approach is rising. India's citizen-focused efforts — like RBI's cyber education in local languages — mirror global shifts, seen in regulations such as the EU's DORA and New York's cybersecurity rules, all aiming to safeguard consumers and promote digital resilience and awareness.

Table 1: Select Comparative Legal Measures

Aspect	**India (2023–24)**	**International Example**
CBDC Legal Status	RBI Act amended to include digital currency as legal tender. Pilot e-Rupee launched; no separate CBDC Act.	EU: Proposed Digital Euro Regulation to give CBDC legal tender status. China: PBOC regulations treat e-CNY as legal tender, banned private crypto.
Cryptocurrency Law	No ban; 30% tax on crypto gains (since 2022) and 1% TDS. Crypto under PMLA for AML compliance. Draft prohibitory law pending (not enacted).	China: All crypto transactions illegal by central directive. EU: Regulated via **MiCA Regulation 2023** (licensing and reserve requirements for crypto-assets). US: No federal law; SEC/CFTC use securities and commodities laws to regulate.
Cybercrime Legislation	IT Act 2000 (amended 2008) in force; new Digital India Act in drafting (focus on intermediary liability, new offences). New criminal code (BNS 2023) explicitly covers cyber fraud and identity theft. Special cyber police stations operational.	EU: Budapest Convention framework (most EU states); NIS2 Directive for network security. UK: Computer Misuse Act + Data Protection Act. Singapore: Computer Misuse and Cybersecurity Acts (strict penalties, proactive cyber defense). Many countries updating laws for cyberbullying, stalking, etc., similarly to India's efforts.
Data Protection	Digital Personal Data Protection Act, 2023 implemented (consent-based, rights granted, heavy fines). Repeals older provisions (IT Act 43A). Government can exempt agencies on security grounds.	EU: GDPR (2018) with strong individual rights and independent regulators. Brazil: LGPD (inspired by GDPR). China: Personal Information Protection Law (2021) with strict consent requirements and data localization (China's approach is more state-controlled but with severe penalties for companies).

Financial Cybersecurity	RBI Master Directions 2023 on IT Governance for banks; CERT-In rules for breach reporting. RBI requires 2FA for payments, banks liable for unauthorised transactions if not customer's fault. National cyber strategy in draft.	US: NY DFS Cyber Regs (2017) for financial firms; EU: DORA (2022) for finance sector cyber resilience; Global: Basel Committee guidelines on operational risk. Many jurisdictions mandate 2FA and have deposit protection for fraud. National cybersecurity strategies (e.g., France's, Australia's updated in 2023) emphasize critical infrastructure protection similar to India's approach on payment systems.

Table 1: Comparison of key legal and regulatory measures in India vs. other jurisdictions (EU, US, China, etc.) in areas of digital currency and cybersecurity.

India is largely aligning with global trends in digital regulation by establishing a legal foundation for its Central Bank Digital Currency (CBDC), enhancing oversight of cryptocurrencies, implementing data protection laws, and modernizing cyber legislation. However, the true test lies in execution. Countries with robust institutions—such as the EU and some Asian nations—tend to enforce such regulations effectively. For India, ensuring the new Data Protection Board and cybercrime enforcement bodies are adequately resourced and independent will be essential for successful implementation. A noteworthy global shift is the adoption of "human-centric digital laws." The EU, for instance, incorporates privacy by design and accessibility into CBDC planning, ensuring usability for all, including the elderly and disabled. India reflects a similar ethos through its focus on financial inclusion via tools like the e-Rupee and UPI, as well as consumer support systems like helpline 1930 and the RBI ombudsman. Future legislation could benefit from embedding stronger user rights, much like the GDPR or financial consumer rights frameworks in other countries. India's 2024 anti-money laundering (AML) regulations for crypto have improved its capacity for international cooperation in investigations. As a G20 leader in 2023, India also championed coordinated virtual asset regulation and secure cross-border payments. In summary, India's evolving digital legal framework mirrors a global push to balance innovation with risk, tailored to national needs and scale.

6. Conclusion and Recommendations:

The year 2024 marked a pivotal chapter in India's legal response to the opportunities and threats of digital finance. Through a series of legislative and regulatory actions – from the statutory enshrinement of the e-Rupee in the RBI Act, to the strengthening of cyber offence laws, to the long-awaited operationalization of a comprehensive Data Protection Act – India has signaled its commitment to securing the digital payment ecosystem with a human-centric focus. The analysis in this paper illustrates that India is erecting a multi-layered legal edifice to protect the e-Rupee and broader fintech innovations from cybercrime, fraud, and misuse of personal identity. This includes not only headline laws and amendments but also crucial subordinate regulations and institutional measures aimed at effective enforcement.

Strengths of the current trajectory: Many of the moves in 2024 fill gaps that existed in the legal framework. The recognition of digital currency as legal tender removed any doubt about the RBI's authority, enabling vigorous rollout of the e-Rupee. Cybercrime provisions in the new penal code acknowledge modern realities, which should aid prosecutions. The DPDP Act brings India into the club of nations with a dedicated data privacy law, enhancing user trust. Additionally, the cooperative stance between regulators (RBI, MeitY, MHA) – visible in joint efforts like the I4C reporting system and RBI's involvement in the national cyber strategy – exemplifies a holistic approach. The focus on user awareness and grievance redress (e.g., fraud helplines, ombudsmen schemes) underlines that laws are being paired with ground-level mechanisms to truly be human-centric.

Addressing weaknesses and loopholes: Despite notable advancements, several weaknesses remain within India's digital regulatory framework. One key issue is the fragmentation of laws, which may cause overlap or ambiguity—cybercrimes, for instance, might fall under both the IT Act and IPC/BNS, necessitating effective coordination between enforcement bodies like the police and the Data Protection Board, especially in data breach cases involving criminal activity. Questions also persist about the constitutional validity of some elements, such as the broad exemptions granted in the DPDP Act or anticipated content regulation under the forthcoming Digital India Act. To avoid repeating past legal missteps (like the invalidation of Section 66A), new laws must respect constitutional guarantees, particularly concerning privacy and free speech. Incorporating sunset clauses or mandatory reviews in new legislation could help maintain legal relevance and human rights compliance in a rapidly evolving digital environment. Another concern is the lack of a clear liability framework for users of the e-Rupee. In the event of wallet breaches or fund loss, user compensation remains undefined. The

RBI should issue specific consumer protection norms for CBDCs, similar to those for electronic banking. Moreover, while the DPDP Act governs private data use, government surveillance practices remain under outdated colonial laws. A modern, rights-respecting surveillance law with oversight mechanisms would complement data protection efforts.

International alignment: India should further align with international frameworks such as the Budapest Convention to enhance cross-border cybercrime cooperation. Through platforms like the G20 and BIS, India can advocate for global standards ensuring security and interoperability of digital currencies, reinforcing both national and international digital resilience.

Human-centric design and education: Legislation alone is not a panacea. A recurring theme is that a human-centric approach means designing systems and processes that are intuitive and secure by default. For the e-Rupee, this could mean RBI and banks emphasizing secure design (for example, wallets that require biometric unlock, and features that allow users to set spending limits or time locks to mitigate misuse). The law should encourage such design by possibly providing guidelines or model standards. Additionally, legal mandates for digital literacy programs could be considered – perhaps as part of Corporate Social Responsibility (CSR) for financial institutions or as government initiatives – because an informed user base is the first line of defense against cyber fraud. India's sheer scale requires that hundreds of millions of new digital users be educated on basic cyber hygiene (not sharing OTPs, recognizing phishing, etc.). This could be achieved by integrating such awareness in school curricula and public campaigns, which the law can indirectly support (for instance, the IT Ministry can be tasked under the new Act to run such programs).

Future outlook: The legislative trends of 2024 are just the beginning. We anticipate that in 2025 and beyond, the following may occur: the Digital India Act will likely be introduced, bringing in a fresh regulatory framework for emerging tech (possibly including AI ethics, something hinted by officials) [33]. The DPDP Act's effectiveness will be tested in landmark cases – those outcomes may prompt amendments or clearer rules (especially around harm compensation and scope of exemptions). The e-Rupee might move from pilot to a broader phase, in which case RBI could request further legislative support if needed (though current laws suffice, unforeseen issues might call for tweaks – for example, a law to prevent the e-Rupee from being refused by any merchant, or to criminalize counterfeiting of CBDC, etc.).

Recommendations: In light of the above analysis, this paper makes a few key recommendations:

- Layered Traceability and Privacy-Conscious Anonymity: Adopt a graded traceability framework tailored to the scale and risk level of transactions. Low-value payments could retain minimal traceability to uphold user confidentiality, whereas high-value or potentially suspicious transactions should be subjected to stricter oversight. This strategy, known as "managed anonymity," offers a balanced model that honors the privacy rights safeguarded under Article 21 of the Indian Constitution while enhancing regulatory monitoring. To reinforce this approach, the Digital India Act must be enacted with precision, ensuring it closes regulatory loopholes (such as those involving AI misuse, IoT vulnerabilities, and ambiguous cybercrime definitions) without infringing on civil liberties. Moreover, strengthening data privacy protections under the Digital Personal Data Protection (DPDP) Act-including provisions for victim compensation and enhanced autonomy for the Data Protection Board-would complement managed anonymity by increasing public trust in digital finance systems.

- Integrated Digital Identity for Safer Financial Ecosystems: As India pivots toward a digital and cashless economy with the adoption of the E-Rupee, it becomes essential to ensure that individual identity remains consistent and verifiable across bank accounts, mobile numbers, and Aadhaar credentials. Integrating Aadhaar authentication with mobile verification (under TRAI's purview) and banking KYC norms will create a unified digital identity system. This will significantly curtail identity-related frauds, unauthorized access, and financial exploitation, thereby boosting public confidence in digital financial services.
  1. To operationalize this vision, three key measures are vital: Unified Identity Framework: Establish interoperable verification standards linking Aadhaar, mobile numbers, and banking credentials. A coordinated verification effort involving TRAI, UIDAI, and financial institutions can deter impersonation and fraudulent activities.
  2. Multi-Factor Authentication Using Aadhaar: Require Aadhaar-based OTP validation / Face recognition for opening new accounts or executing high-value digital transactions, ensuring only the rightful owner can authorize financial activity.
  3. Inclusive Digital Empowerment: Design transparent and accessible identity verification systems to protect marginalized populations from fraud, allowing them to safely participate in the digital economy.

- Enact the Digital India Act with caution and precision: Focus on filling gaps (like comprehensive definitions of new cybercrimes, regulation of AI and IoT security, intermediary liability framework) while ensuring consistency

with fundamental rights. Consider retaining safe harbor for platforms with duties rather than imposing outright content control that could be abused. Include provisions to strengthen critical infrastructure security, perhaps mandating periodic security audits for payment systems and fintech platforms.

- Strengthen the Data Protection regime: Amend the DPDP Act in the future to introduce a mechanism for individual compensation (even if through an adjudicatory tribunal or expanded powers of the Data Protection Board to direct compensation to victims of data breaches). This will reinforce trust that individuals have recourse if their personal/financial data is compromised. Also, ensure the Data Protection Board is independent and well-resourced.

- Augment law enforcement capabilities: Pass necessary administrative orders or amendments to empower law enforcement for cybercrime – for example, faster warrant procedures for electronic evidence, legal recognition for digital evidence chains (something the new Evidence Act draft is likely addressing). Expand training and hiring of cybercrime investigators. On a legislative front, consider special cyber courts in metros with judges trained in technology, to speed up trials of complex cyber fraud cases.

- Promote public-private collaboration: The laws should encourage information sharing between government and the private sector. For instance, a legal safe harbor for banks that share fraud intelligence with each other (so that scammers blacklisted by one bank don't simply hop to another). Some of this can be done via RBI directives, but a statutory backing could amplify it.

- Regular review of progress: Perhaps mandate that a Joint Parliamentary Committee on Digital Economy review the impact of these laws annually for the first few years. This committee can take inputs from regulators, industry, and citizen groups to recommend fine-tuning. The digital realm evolves quickly, and legislative agility is needed – a structured review process can prevent the laws from becoming quickly outdated.

In conclusion, India's digital legal landscape underwent a transformative shift in 2024, laying a robust foundation for a secure, inclusive, and future-ready financial ecosystem. The strategic recognition of the e-Rupee within the statutory framework, coupled with strengthened cybercrime laws and the rollout of the Data Protection Act, signals a deliberate move toward a human-centric, rights-based approach to digital finance. What sets India's trajectory apart is the integration of legislative ambition with institutional coordination, citizen awareness, and infrastructural readiness.

However, sustaining this momentum will require more than legal enactments—it demands continuous refinement, effective enforcement, and broad-based collaboration between the state, industry, and civil society. Closing the remaining gaps—such as overlapping jurisdictions, undefined user liabilities in CBDC usage, and the absence of updated surveillance safeguards—must be prioritized. Equally critical is the enactment of the Digital India Act with constitutional fidelity and technological foresight, alongside necessary reforms to the DPDP Act and cyber enforcement capacities.

If India maintains a clear commitment to privacy, innovation, and user empowerment, it has the potential to emerge not just as a digital economy leader, but as a global model for balancing fintech innovation with democratic values. The legislative progress of 2024 is not an endpoint but a beginning—one that must be advanced through vigilant oversight, dynamic regulatory response, and ongoing dialogue. The success of this vision will ultimately rest on how effectively the laws translate into secure experiences for citizens navigating an increasingly digital financial world.

References:

1. Reserve Bank of India, India, "Digital Rupee (e₹) – FAQs" (2025), Available at: https://www.rbi.org.in/commonman/English/scripts/FAQs.aspx?Id=3686#:~:text=17,tender (Last Visited on March 27, 2025).

2. Manish Mimani, Founder & CEO, Protectt.ai, "Why digital privacy and security are critical for CBDC e-rupee's success, and winning customers trust" (2023), Available at: https://www.expresscomputer.in/artificial-intelligence-ai/why-digital-privacy-and-security-are-critical-for-cbdc-e-rupees-success-and-winning-customers-trust/100700/#:~:text=It%20is%20in%20this%20context,secure%20information%2C%20and%20steal%20money (Last visited on March 27, 2025)

3. Indian Institute of Legal Studies, "Critical Analysis Of The Bharatiya Nyaya Sanhita: A New Era For Indian Criminal Law?" Available at: https://www.iilsindia.com/blogs/critical-analysis-of-the-bharatiya-nyaya-sanhita-a-new-era-for-

indian-criminal-law/ (Last visited on March 27, 2025)

4. THE FINANCE BILL, 2022, "AS INTRODUCED IN LOK SABHA", Available at: https://www.indiabudget.gov.in/budget2022-23/doc/Finance_Bill.pdf#:~:text=digital%20form%20of%20bank%20notes,issued%20in%20digital%20form%20by (Last visited on March 27, 2025)

5. Reserve Bank of India, India, "Digital Rupee (e₹) – FAQs" (2025), Available at: https://www.rbi.org.in/commonman/English/scripts/FAQs.aspx?Id=3686#:~:text=17,tender (Last Visited on March 27, 2025).

6. Wikipedia, "Concept stage" (2022), Available at: https://en.wikipedia.org/wiki/Digital_rupee#:~:text=2022%20enacted%20with%20amendments%20in,domestic%20and%20cross%20border%20payment (Last Visited on March 27, 2025)

7. Manish Mimani, Founder & CEO, Protectt.ai, "Dilemma of the need for technology and cybersecurity" (2023), Available at: https://www.expresscomputer.in/artificial-intelligence-ai/why-digital-privacy-and-security-are-critical-for-cbdc-e-rupees-success-and-winning-customers-trust/100700/#:~:text=It%20is%20in%20this%20context,secure%20information%2C%20and%20steal%20money (Last visited on March 27, 2025)

8. Reserve Bank of India, India, "Digital Rupee (e₹) – FAQs" (2025), Available at: https://www.rbi.org.in/commonman/English/scripts/FAQs.aspx?Id=3686#:~:text=17,tender (Last Visited on March 27, 2025).

9. Moneylife, "RBI Issues New Directions to Banks, NBFCs on IT Governance & Cybersecurity" (2023), Available at: https://www.moneylife.in/article/rbi-issues-new-directions-to-banks-nbfcs-on-it-governance-and-cybersecurity/72528.html#:~:text=The%20Reserve%20Bank%20of%20India,safeguard%20the%20interests%20of%20customers (Last Visited on March 30, 2025).

10. Manish Mimani, Founder & CEO, Protectt.ai, "Dilemma of the need for technology and cybersecurity" (2023), Available at: https://www.expresscomputer.in/artificial-intelligence-ai/why-digital-privacy-and-security-are-critical-for-cbdc-e-rupees-success-and-winning-customers-trust/100700/#:~:text=It%20is%20in%20this%20context,secure%20information%2C%20and%20steal%20money (Last visited on March 27, 2025)

11. Wikipedia, "Concept stage" (2022), Available at: https://en.wikipedia.org/wiki/Digital_rupee#:~:text=2022%20enacted%20with%20amendments%20in,domestic%20and%20cross%20border%20payment (Last Visited on March 27, 2025)

12. Hardeep Sachdeva, "The Finance Bill, 2022 – A Legal Recognition to Virtual Currencies in India?" (2022), available at: https://www.azbpartners.com/bank/the-finance-bill-2022-a-legal-recognition-to-virtual-currencies-in-india/#:~:text=In%20light%20of%20the%20above%2C,legality%20of%20cryptocurrencies%20in%20India (Last Visited on March 27, 2025)

13. Financial Express, "Will not rush in bringing Digital India Act: MeitY secretary" (2025), Available at: https://www.financialexpress.com/life/technology-will-not-rush-in-bringing-digital-india-act-meity-secretary-3708673/ (Last Visited on March 27, 2025)

14. Nadeem Inamdar, "Lt Gen Rajesh Pant (retd), national cyber security coordinator, National Security Council Secretariat, said on Monday said that the National Cyber Security Strategy 2023 is in final stages of approval" (2023), Available at: https://www.hindustantimes.com/cities/pune-news/national-cyber-security-strategy-2023-to-be-released-soon-101686596627065.html (Last Visited on March 27, 2025)

15. Shouvik Das, "Govt prepares new cyber security policy to beat malware attacks" (2023), Available at: https://www.livemint.com/technology/govt-prepares-new-cyber-security-policy-to-beat-malware-attacks-11686717816691.html (Last Visited on March 27, 2025)

16. Indian Institute of Legal Studies, "Critical Analysis Of The Bharatiya Nyaya Sanhita: A New Era For Indian Criminal Law?", Available at: https://www.iilsindia.com/blogs/critical-analysis-of-the-bharatiya-nyaya-sanhita-a-new-era-for-indian-criminal-law/ (Last visited on March 27, 2025)

17. Manisha Singh, Srinjoy Banerjee, "Cybersecurity Laws and Regulations India 2025" (2024), Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india#:~:text=fined%20up%20to%20Rs%20200%2C000%2C,fraudulent%20purposes%2C%20financial%20gain%2C%20or (Last visited on March 27, 2025)

18. PRS Legislative Research, "The Bharatiya Nyaya (Second) Sanhita, 2023" (2023), Available at: https://prsindia.org/billtrack/the-bharatiya-nyaya-second-sanhita-2023#:~:text=to%20threaten%20the%20unity%2C%20integrity%2C,death%2C%20and%20with%20a%20fine (Last visited on March 27, 2025)

19. Indian Institute of Legal Studies, "Critical Analysis Of The Bharatiya Nyaya Sanhita: A New Era For Indian Criminal Law?", Available at: https://www.iilsindia.com/blogs/critical-analysis-of-the-bharatiya-nyaya-sanhita-a-new-era-for-indian-criminal-law/ (Last visited on March 27, 2025)

20. Business-standard, "Here is how much Indians lost to cyber frauds between Jan and Apr of 2024" (2024), Available at: https://www.business-standard.com/india-news/here-is-how-much-indians-lost-to-cyber-frauds-between-jan-and-apr-of-2024-124052700151_1.html Last visited on March 27, 2025)

21. Times of India, "India saw 129 cybercrimes per lakh population in 2023" (2024), Available at: https://timesofindia.indiatimes.com/india/india-saw-129-cybercrimes-per-lakh-population-in-2023/articleshow/106524847.cms Last visited on March 27, 2025)

22. Times of India, "India saw 129 cybercrimes per lakh population in 2023" (2024), Available at: https://timesofindia.indiatimes.com/india/india-saw-129-cybercrimes-per-lakh-population-in-2023/articleshow/106524847.cms Last visited on March 27, 2025)

23. Nishith Desai Associates, "I ndia's Digital Personal Data Protection Act, 2023: History in the Making" (2023), Available at: https://www.nishithdesai.com/NewsDetails/10703#:~:text=,specifically%2C%20the%20SPDI%20Rules Last visited on March 27, 2025)

24. Linklaters, "Data Protected - India" (2024), Available at: https://www.linklaters.com/en-us/insights/data-protected/data-protected---india#:~:text=When%20the%20DPDP%20Act%20comes,72A%20of%20the%20Information, Last visited on March 29, 2025)

25. Linklaters, "Data Protected - India" (2024), Available at: https://www.linklaters.com/en-us/insights/data-protected/data-protected---india#:~:text=When%20the%20DPDP%20Act%20comes,72A%20of%20the%20Information, Last visited on March 29, 2025)

26. Mihir R, "Digital Personal Data Protection Act, 2023: A missed opportunity for horizontal equality" (2023), Available at: https://www.scobserver.in/journal/digital-personal-data-protection-act-2023-a-missed-opportunity-for-horizontal-equality/#:~:text=suggested%20in%20the%202019%20draft,Data%20Protection%20Authority%20of%20India Last visited on March 29, 2025)

27. Manish Mimani, Founder & CEO, Protectt.ai, "Why digital privacy and security are critical for CBDC e-rupee's success, and winning customers trust" (2023), Available at: https://www.expresscomputer.in/artificial-intelligence-ai/why-digital-privacy-and-security-are-critical-for-cbdc-e-rupees-success-and-winning-customers-trust/100700/#:~:text=It%20is%20in%20this%20context,secure%20information%2C%20and%20steal%20money (Last visited on March 27, 2025)

28. Lakshikumaran Sridharan Attorneys, "Money laundering provisions to apply to Cryptocurrency sector" (2023), Available at: https://www.lakshmisri.com/newsroom/news-briefings/money-laundering-provisions-to-apply-to-cryptocurrency-sector/# (Last visited on March 28, 2025)

29. Wikipedia, Digital rupee (2023), Available at:

https://en.wikipedia.org/wiki/Digital_rupee#:~:text=match%20at%20L688%2036.%20,Information%20Technology%2C%20Government%20of%20India (Last visited on March 28, 2025)

30. European Parliament, "Digital euro package [EU Legislation in Progress] (2023)", Available at: https://epthinktank.eu/2023/09/18/digital-euro-package-eu-legislation-in-progress/#:~:text=Digital%20euro%20package%20,framework%20for%20a%20digital%20euro (Last visited on March 29, 2025)

31. Library of Congress, "China: Central Bank Issues New Regulatory Document on Cryptocurrency Trading" (2021), Available at: https://www.loc.gov/item/global-legal-monitor/2021-10-13/china-central-bank-issues-new-regulatory-document-on-cryptocurrency-trading/#:~:text=The%20new%20PBOC%20circular%20declares,selling%20cryptocurrencies%20as%20a (Last visited on March 29, 2025)

32. Hogan Lovells, "China's Sovereign Digital Currency and Electronic Payment (DC/EP): a Hong Kong Perspective" (2021), Available at: https://www.hoganlovells.com/en/publications/chinas-sovereign-digital-currency-and-electronic-payment-dcep-a-hong-kong-perspective_1#:~:text=China%27s%20Sovereign%20Digital%20Currency%20and,legal%20tender%20in%20Mainland%20China (Last visited on March 29, 2025)

33. Financial Express, "Will not rush in bringing Digital India Act: MeitY secretary" (2025), Available at: https://www.financialexpress.com/life/technology-will-not-rush-in-bringing-digital-india-act-meity-secretary-3708673/ (Last Visited on March 27, 2025)