

# **DIGITAL TRANSACTIONS AND THE RISE OF CYBERCRIMES: TESTING THE READINESS OF THE INDIAN LEGAL STRUCTURE**

~ Dwija Vasavada & Diya Gohil <sup>1</sup>

## **ABSTRACT**

*In the era of digitalization, the Indian economy has witnessed a major upturn with the help of breakthrough policies and digitally-backed structures that have eased the lives of millions of nationals of the country. With a swipe, a hefty sum of money can be transferred from one remote area of the county to another within a fraction of a second. This trend in the techno- digital world has made everyone well-versed in terms like "e-banking," "e-commerce," "e-networking," etc., wherein the angle of preference or choice is greatly bent towards the mode that is easily accessible and attainable. But with the increase in the number of users of such digitally driven systems, it is equally important to regulate such platforms by framing stringent laws to protect the fundamental right to privacy of the users against the misuse of the sensitive information that has been shared by them with a sense of utmost reliance. Therefore, considering all the outlining aspects of an economy that is at the peak of automation, the authors in this article aim to deeply analyze the legalities that revolve around the digital economy concerning the digital payment systems of the country to identify the drawbacks in the governance of such laws that regulate it. The article begins with an overview of the online transaction system, which has flourished primarily since the pandemic, and then sheds some light on the potential cybercrimes that have been increasing with technological advancement. It further discusses the current legal system by identifying specific loopholes, and lastly, the authors provide relevant findings and suggestions and analyze international jurisdictions that have been in conflict with the "digitalization of crimes" to counter the menace of the spurt of cybercrimes and the drawbacks of the Indian legal structure.*

---

<sup>1</sup> The authors are in their 2<sup>nd</sup> Year at Gujarat National Law University and United World School of Law.

## I. UNDERSTANDING E-TRANSACTIONS AND THE INDIAN DIGITAL ECONOMY

It should not come as a surprise that the world's fifth-largest economy is leading and advancing global digital wealth, but what is noteworthy is the significant surge that has occurred in such a short span of time. The term "digital economy" describes how the digital revolution is replacing conventional brick-and-mortar activities. The transformation has not only altered people's fundamental way of life but has also played an important role in raising their standards of living. Many sectors of the economy have witnessed notable changes as a result of digital advancement, including medicine, education, banking, and the service sector, among many others.

The Government of India launched the Digital India Campaign in 2015 to empower the nation digitally and improve the online infrastructure of the Indian economy. The Unified Payments Interface (UPI) portal was created by the National Payments Corporation of India (NPCI), an initiative of the Reserve Bank of India, to expedite and streamline digital transactions. The portal facilitates interbank real-time transactions via mobile applications such as Bharat Interface for Money (BHIM), Google Pay, Paytm, PhonePe, and others. Even in the midst of the Indian economy's deteriorating conditions, this inclusive digital model of India contributed to closing the digital divide and bringing the advantages of technology to all facets of the population. Hence, it is important to use digitization as the primary factor of production to establish a sound digital economy.

The era of digital transactions in India began in 1996 when banks started offering online banking services through electronic banking at their branches. Later, as more banks launched net banking services, the trend accelerated. Technology was already playing a bigger role in the workforce, but it was not until the pandemic that a complete reliance on the digital economic setup was seen. Due to the impact of COVID-19, the banking, education, healthcare, and food delivery sectors have grown rapidly. And since then, there has been a significant increase in the number of users of "e-transactions" in India.

The outbreak of the novel coronavirus and the prohibition against in-person business meetings significantly hastened the adoption of these technologies. With the rise in the number of coronavirus cases, digital transactions have become more common. From a tea vendor to a large corporation, everyone has recognized the value of digitization and, as a

## **Digital Transactions And The Rise Of Cybercrimes: Testing The Readiness Of The Indian Legal Structure**

result, has adopted the digital method. In light of this, it can be said that even though the nationwide lockdown was upsetting, Indian electronic payment systems have turned out to be a blessing in disguise.

### **II. CYBERCRIMES IN INDIA AND THE GROWTH TRAJECTORY**

The prevalence of cybercrime has indeed increased with the rise of digital technology. The transition from traditional work culture to digital operations has brought numerous benefits and innovations, but it has also introduced new vulnerabilities and threats to cybersecurity. The interconnected nature of digital systems and the growing reliance on technology for various aspects of our lives have provided cybercriminals with more opportunities to exploit weaknesses and carry out malicious activities. These activities can range from stealing sensitive personal information and financial data to launching large-scale cyberattacks on organizations and even governments.

The history of cybercrime in India can be traced back to the early days of the Internet. In the late 1990s and early 2000s, India's internet penetration was still relatively low, and cybercrime was largely limited to hacking and unauthorized access to computer systems. These early cybercriminals were often motivated by curiosity or a desire to showcase their technical skills. India's internet usage increased along with the rise in cybercrime incidents.

In the mid-2000s, incidents of online fraud and identity theft started to increase. These crimes were frequently carried out by lone perpetrators or small groups using simple tools and techniques. In the late 2000s and early 2010s, as social media and mobile technology grew in popularity, a new set of cybercrime challenges emerged. Social media platforms became breeding grounds for cyberbullying, online harassment, and the spread of misinformation.

In 2013, India witnessed its first cybercrime conviction following a complaint filed by Sony India Private Ltd. The case of Sony Sambandh<sup>2</sup> involved a fraudulent transaction made on a website targeting non-resident Indians. The accused gained access to an American national's credit card number while working at a call centre and misused it on the website to purchase a Sony television set and cordless headphones. The company delivered the products to the accused, but it was later discovered that the transaction was unauthorized. Sony lodged a

---

<sup>2</sup> Avni Mishra, *A primer on cybercrimes*, 2 JUS CORPUS LAW J. 12 (2021), <https://www.juscorpus.com/wp-content/uploads/2021/09/3.-Avni-Mishra.pdf>.

complaint, and the Central Bureau of Investigation (CBI) registered a case under Sections 418<sup>3</sup>, 419<sup>4</sup>, and 420<sup>5</sup> of the Indian Penal Code, 1860.

The Court found the accused guilty and convicted him under the relevant sections of the Indian Penal Code, 1860<sup>6</sup>, marking the first conviction in a cybercrime case in India. Despite this, considering his young age and first-time offense, the Court released the accused on probation for one year. The judgment holds significance as it demonstrates the effective application of the Indian Penal Code to certain cybercrimes not covered by the Information Technology Act, of 2000<sup>7</sup>, and sends a strong message that the law cannot be disregarded.

In another such incident, in August 2018, Cosmos Bank in Pune, India, fell victim to a bold cyberattack in which Rs 94 crores were stolen. The hackers managed to breach the bank's main server and transfer the stolen funds to a bank in Hong Kong. Additionally, they infiltrated the ATM server to gather information from VISA and Rupay debit cards. The attack targeted the switching system, which acts as a link between the centralized system and the payment gateway. This prevented the bank and account holders from detecting fraudulent money transfers. This attack was unique and notable as it involved the first malware attack that disrupted all communication between the bank and the payment gateway, enabling the hackers to execute their fraudulent activities without raising suspicion<sup>8</sup>.

These cases highlight the evolving sophistication of cybercrime in India and the need for robust cybersecurity measures to protect individuals, organizations, and the government. As technology continues to advance, it is crucial to stay vigilant and adapt security frameworks to address emerging cyber threats.

With the rapid advancement of technologies like artificial intelligence, blockchain, and the metaverse, cybercrime has also become more sophisticated and organized. Hackers are leveraging these technologies to commit online crimes and exploit vulnerabilities in digital systems.

The use of artificial intelligence by cybercriminals is a concerning trend. They can employ AI to enhance the effectiveness of their attacks, generate targeted phishing emails, spread

---

<sup>3</sup> The Indian Penal Code, 1860, § 418, No. 45, Acts of Parliament, 1860 (India).

<sup>4</sup> The Indian Penal Code, 1860, § 419, No. 45, Acts of Parliament, 1860 (India).

<sup>5</sup> The Indian Penal Code, 1860, § 420, No. 45, Acts of Parliament, 1860 (India).

<sup>6</sup> The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).

<sup>7</sup> Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

<sup>8</sup> About Us et al., *Important Cyber Law Case Studies*, Cyber Laws & Information Security Advisors 4 (2019), <https://www.cyberalegalservices.com/detail-casestudies.php>.

## **Digital Transactions And The Rise Of Cybercrimes: Testing The Readiness Of The Indian Legal Structure**

malware, and collect valuable information by leveraging stolen personal information or open-source data. This demonstrates the need for robust cybersecurity measures to counteract the malicious use of AI.

Espionage and cyberattacks pose significant threats to national security and diplomatic relations for governments. As the concept of Central Bank Digital Currency (CBDC) gains attention, there are specific risks associated with third-party involvement in its implementation. Professionals need to understand the evolving landscape of digital finance to mitigate these risks and protect financial systems from cybercriminals.

The rise of e-currencies and digital payment methods has also led to an exponential increase in digital payment and banking fraud. Cybercriminals target online banking, impersonate bank officials, and exploit vulnerabilities to dupe customers and steal their personal and financial information. The occurrence of frauds involving Aadhar scams and online scams demonstrates the need for improved security in digital transactions and banking services.

Government portals and websites that handle sensitive data are also at risk of being hacked and misused. Cybercriminals can exploit vulnerabilities in these platforms and commit fraud involving debit and credit cards, digital signatures, and electronic contracts. This poses a threat not only to security but also to the confidence of individuals who rely on online activities.

To combat cybercrime effectively, India's legal and security frameworks must keep pace with the evolving landscape of technology. It is crucial to implement robust measures to control and monitor digital platforms, ensuring adherence to cybersecurity standards for privacy and safety. By prioritising cybersecurity and adopting proactive measures, individuals and organisations can mitigate the risks posed by cybercrime and protect sensitive information online.

### **III. DEVELOPMENT OF LAWS TO REGULATE E-TRANSACTIONS AND POTENTIAL CRIMES**

In 2022, India clocked about 70 billion payment transactions, which is the highest in the world, and research by NPCI and People Research on India's Consumer Economy showed that one-third of Indian households are now using digital payments in one way or another<sup>9</sup>.

---

<sup>9</sup> Mahua Venkatesh, *India tops world ranking in digital payments*, Indianarrative, Oct. 19, 2022, <https://www.indianarrative.com/economy-news/india-tops-world-ranking-in-digital-payments-62451.html>.

Such an increase in digital payments and internet penetration is unavoidable, but with a growing concern about cybercrime in India and around the world, it is essential to formulate policies and enact legislation that prevent the spread of such offenses.

To prevent the abuse of one's integrity, financial institutions that operate digitally need effective cyber laws. As a result, it becomes increasingly important for the Indian legal system to evolve continuously to meet the challenges posed by cybercrime and keep up with its changing nature. In India, there are several cyber laws and regulations in place to curb and regulate digital transactions and potential Internet crimes. Here are some key pieces of legislation that address these issues:

1. **Information Technology Act, 2000<sup>10</sup> (IT Act):** This is the primary legislation governing cyber activities in India. The statute establishes the rules for data protection and aims to give people more control over their personal information, including the right to be forgotten. It provides legal recognition for electronic transactions, digital signatures, and electronic records. The IT Act also defines various cybercrimes and their penalties, such as unauthorized access, hacking, identity theft, phishing, cyberstalking, and distributing obscene materials online.
2. **The Indian Penal Code, 1860<sup>11</sup> (IPC):** While not specific to cybercrimes, the IPC has provisions that can be applied to online offenses. Sections such as 419<sup>12</sup> (cheating by personation), 463<sup>13</sup> (forgery), 464<sup>14</sup> (making a false document), 465<sup>15</sup> (forgery), and others can be invoked for cybercrimes.
3. **The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021<sup>16</sup>:** These rules, issued under the IT Act, govern the functioning of intermediaries, social media platforms, and digital content providers. They prescribe obligations such as content takedown, the appointment of grievance officers, and disclosure of the originator of objectionable content.

---

<sup>10</sup> Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

<sup>11</sup> The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).

<sup>12</sup> The Indian Penal Code, 1860, § 419, No. 45, Acts of Parliament, 1860 (India).

<sup>13</sup> The Indian Penal Code, 1860, § 463, No. 45, Acts of Parliament, 1860 (India).

<sup>14</sup> The Indian Penal Code, 1860, § 464, No. 45, Acts of Parliament, 1860 (India).

<sup>15</sup> The Indian Penal Code, 1860, § 465, No. 45, Acts of Parliament, 1860 (India).

<sup>16</sup> The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

## **Digital Transactions And The Rise Of Cybercrimes: Testing The Readiness Of The Indian Legal Structure**

4. **The Payment and Settlement Systems Act, 2007<sup>17</sup>:** This statute governs digital payments and provides the legal framework for electronic funds transfer, the regulation of payment systems, and the establishment of payment system operators in India.
5. **The Reserve Bank of India (RBI) Regulations:** The RBI issues various regulations to govern digital transactions, including guidelines for electronic wallets (Prepaid Payment Instruments), online banking, and online payment gateways such as Know Your Customer (KYC) Guidelines<sup>18</sup>, Two-Factor Authentication (2FA), etc. These regulations aim to ensure the security and integrity of digital transactions.
6. **The Aadhaar Act, 2016<sup>19</sup>:** The Aadhaar Act establishes a unique identification system in India called Aadhaar, which provides a unique identification number to residents. It governs the collection, storage, and usage of Aadhaar-related data and aims to prevent identity-related fraud and misuse.
7. **The Digital Personal Data Protection Bill, 2022<sup>20</sup>:** The Union Government of India has introduced a revised version of the personal data protection bill, now known as the Digital Personal Data Protection Bill, 2022. Unlike the previous version, this bill allows for cross-border data transfers, instead of mandating local storage of data within India. It takes a more flexible approach to data localization requirements and permits data transfers to specific international destinations, potentially promoting trade agreements between countries. Additionally, the bill acknowledges the right to post-mortem privacy, allowing individuals to withdraw consent even after their death, a provision that was missing in the previous 2019 bill but was recommended by the Joint Parliamentary Committee (JPC).

These are some of the key cyber laws and regulations in India that aim to curb and regulate digital transactions and potential Internet crimes. These are put in place to protect individuals from the unauthorized collection, use, and dissemination of their personal information. Data

---

<sup>17</sup> Payment and Settlements System Act, 2007, No. 51, Acts of Parliament, 2007 (India).

<sup>18</sup> Reserve Bank of India, Master Directions on Know Your Customer, RBI/DBR/2015-16/18 (Issued on May 29, 2019).

<sup>19</sup> The Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act, 2016, No. 47, Acts of Parliament, 2016 (India).

<sup>20</sup> Draft Digital Personal Data Protection Bill, 2022, PRS INDIA (2022), <https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022>.

privacy regulations mandate that organizations follow appropriate security measures and procedures to safeguard sensitive personal data or information in accordance with data privacy regulations.

#### IV. CYBERSECURITY IN LINE WITH THE FINTECH SECTOR

The emergence of FinTech (financial technology) in recent years has created new difficulties for data security and privacy. It is of utmost importance for the concerned governing authorities of the respective jurisdictions to make regulations for the same because fintech companies frequently collect and use large amounts of personal and financial data, making them a prime target for fraudsters.

The financial regulatory landscape in India is characterised by fragmentation, with different regulatory bodies overseeing different aspects of the industry. Fintech companies, despite having limited capital, face regulatory risks that could potentially lead to their collapse or dependence on larger institutions. The Reserve Bank of India (RBI), as the central bank, has emphasised its customer-centric approach to regulation. Various regulatory institutions, including the RBI, SEBI, IRDA, the Ministry of Electronics and Information Technology, and the Ministry of Finance, have developed rules and regulations to govern the product offerings of fintech entities.

While the RBI has released a detailed cybersecurity framework<sup>21</sup>, it currently applies only to banks and non-banking financial institutions. The Working Group<sup>22</sup> established by the RBI has identified the need to safeguard customers from unethical practices and the potential stability risks associated with the rapid expansion of digital lending during the pandemic. The group examined issues related to the collaboration between the RBI and other fintech companies offering services such as digital payment systems and "Buy Now, Pay Later" schemes. To protect customer confidentiality and comply with data secrecy obligations, the RBI has issued master directives on the outsourcing of IT services<sup>23</sup> for prepaid payment instructions, and credit-debit cards, which apply to non-banking financial companies (NBFCs) and credit information companies (CICs).

---

<sup>21</sup> Reserve Bank of India, Cyber Security Framework in Banks, (Notified on June 2, 2016).

<sup>22</sup> Reserve Bank of India, Report of the Working Group on digital lending including lending through online platforms and mobile apps, (Issued on November 18, 2021).

<sup>23</sup> Reserve Bank of India, Draft Master Direction on Outsourcing of Information Technology (IT) Services, (Issued on June 23, 2022).

## **Digital Transactions And The Rise Of Cybercrimes: Testing The Readiness Of The Indian Legal Structure**

The regulatory bodies have formulated key rules to effectively regulate fintech companies. The Payment and Settlements Act, 2007<sup>24</sup> (PSS Act) is the principal regulation governing payments in India, encompassing various payment systems such as debit cards, credit cards, smart cards, and money transfer systems. Additionally, the RBI has issued circulars and notifications outlining requirements for data localization and data privacy for Payment Aggregators (PA), while the Insurance Regulatory and Development Authority of India (IRDAI) has published Information and Cyber Security Guidelines<sup>25</sup> for the insurance sector. Regulations related to cyber security are also encompassed under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016<sup>26</sup>, and the Credit Information Companies (Regulation) Act, 2005<sup>27</sup>.

Furthermore, financial authorities have specific rules and directives regarding the maintenance of financial transaction records and customer verification under the Prevention of Money Laundering Act, 2002<sup>28</sup> (PMLA). Authorities like SEBI, RBI, and IRDA have imposed obligations on securities market intermediaries and established guidelines on anti-money laundering and counter-financing of terrorism measures. These regulatory measures aim to ensure the security, privacy, and integrity of financial transactions and protect customers from potential risks in the fintech industry.

While challenges and areas for improvement remain, the regulatory measures implemented aim to strike a balance between promoting innovation and protecting customers. The evolving nature of the fintech industry and advancements in technology call for continuous updates and enhancements to the regulatory framework to address emerging risks and foster a secure and thriving fintech ecosystem in India.

---

<sup>24</sup> Payment and Settlements System Act, 2007, No. 51, Acts of Parliament, 2007 (India).

<sup>25</sup> Insurance Regulatory and Development Authority of India, Guidelines on Information and Cyber Security for insurers, IRDA/IT/GDL/MISC/ 082/04/2017, (Issued on April 7, 2017).

<sup>26</sup> The Aadhaar (Targeted Delivery of Financial and other subsidies, benefits and services) Act, 2016, No. 47, Acts of Parliament, 2016 (India).

<sup>27</sup> The Credit Information Companies (Regulation) Act, 2005, No. 30, Acts of Parliament, 2005 (India).

<sup>28</sup> The Prevention of Money Laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India).

## V. ANALYSIS OF INTERNATIONAL JURISDICTIONS AND THEIR EXPERIENCE WITH FINTECH FRAUDS

Considering that India is the third-largest fintech ecosystem and is among the fastest-growing fintech markets in the world, the Indian fintech industry is envisioned to be valued at around USD 150 billion by 2025<sup>29</sup>. Financial regulators not only in India but around the world recognize the need for innovation and work to support and promote FinTech activities by instituting regulatory virtual spaces because it can be challenging to integrate them into the current regulatory framework.

Not only is the growth of FinTech cybersecurity and fraud taking an upward turn, but new payment systems and instruments have also been found to be compromising the integrity of the market. Regulators must therefore strike the ideal balance between competitive advantages. Risks associated with integrating new technologies with current company models can be mitigated via fintech. As a result, financial services are one of the industries with the most regulation worldwide. Given that there are numerous financial ecosystems around the world, each with varying levels of complexity and regulatory systems, there is no one-size-fits-all solution that will satisfy all stakeholders in every state or work in every country.

Analysing international jurisdictions and their experiences with fintech fraud can provide insights into the challenges and measures taken to address fraudulent activities in the fintech sector. While it's important to note that the situation may vary across countries, here are some notable examples:

**United States:** The United States has seen several cases of fintech fraud, including Ponzi schemes, identity theft, and fraudulent investment schemes. Regulatory bodies like the Securities and Exchange Commission (SEC) and the Consumer Financial Protection Bureau (CFPB) have taken actions to combat fraud in the fintech industry. Enhanced regulations, such as Know Your Customer (KYC) requirements and anti-money laundering measures, have been implemented to mitigate risks.

**United Kingdom:** The UK has experienced various fintech fraud cases, such as payment fraud, phishing attacks, and crowdfunding scams. The Financial Conduct Authority (FCA) regulates fintech activities and has implemented measures to protect consumers and enhance

---

<sup>29</sup> The changing face of financial services: Growth of FinTech in India, Jun. 2022, <https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/publications/the-changing-face-of-financial-services-growth-of-fintech-in-india-v2.pdf>.

## **Digital Transactions And The Rise Of Cybercrimes: Testing The Readiness Of The Indian Legal Structure**

cybersecurity. The UK has also established the National Cyber Security Centre (NCSC) to address cyber threats and provide guidance to businesses, including fintech firms.

**Singapore:** Singapore has witnessed instances of fintech fraud, particularly in areas like peer-to-peer lending and investment scams. The Monetary Authority of Singapore (MAS) regulates fintech activities and has introduced stringent regulations, including robust licensing requirements, mandatory cybersecurity measures, and fraud detection frameworks. The MAS encourages collaborations between fintech companies and financial institutions to enhance fraud prevention measures.

**Australia:** Australia has faced fintech fraud challenges, including identity theft, fraudulent mobile banking apps, and online payment scams. The Australian Securities and Investments Commission (ASIC) oversees the fintech sector and has introduced measures to protect consumers. The ASIC focuses on ensuring compliance with financial regulations, promoting consumer education, and encouraging industry collaboration to combat fraud.

**European Union (EU):** The EU has encountered fintech fraud cases ranging from money laundering to data breaches. The European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) regulate fintech activities within the EU. The EU has introduced the General Data Protection Regulation (GDPR) to protect personal data and implemented anti-money laundering directives to combat financial crimes.

**China:** In contrast, some countries have less robust laws and regulations in place. For example, in China, there is no specific law that governs cyber security in transactions. Instead, companies are expected to abide by general laws and regulations. Such legislation requires companies to implement security measures to protect personal information and report data breaches to the government, but it does not have the same level of fines and penalties for non-compliance as GDPR. However, the region has seen a surge in FinTech frauds, particularly those involving mobile payments. For example, in 2018, China faced a major scam involving mobile payments where consumers were duped into transferring money to fraudsters.

Overall, it can be seen that laws and regulations for transaction-related cyber security vary greatly around the world. Some countries have specific laws and penalties for non-compliance, while others rely on general laws and regulations. Businesses operating internationally should be aware of the different laws and regulations in the countries where

they operate to ensure compliance and protect against cyberattacks and data breaches. Not just businesses, but there have been cases of mass cyberbullying done by one nation against another. Therefore, proper governance of cyber laws is necessary so that national interests are protected.

## VI. CHALLENGES AND DRAWBACKS IN THE FACE OF TRANSITION TO A DIGITAL ENVIRONMENT

In spite of these laws, there are some inadequacies in India's implementation of data privacy measures. These challenges can hinder the effective protection of data privacy and the prosecution of cybercrime.

**1. Lack of awareness and understanding:** Many individuals and organisations are not familiar with their rights and responsibilities under data privacy laws. The IT sector has grown at such a rapid pace that it has become difficult for the masses to adapt to this fast- growing technology. *While the overall literacy rate in the country has to bridge a gap of 25- 30%, digital literacy is almost non-existent among more than 90% of India's population. At the same time, there has been a concerted push towards deeper penetration of the internet, along with the phenomenal increase in smartphone usage.*<sup>30</sup>

This suggests that although there are more people using technology and the internet, they are still largely ignorant of the necessary safety and security precautions. This lack of awareness can discourage people from reporting incidents and hinder the effective development, comprehension, implementation, and compliance with data privacy regulations.

**2. Insufficient technical know-how:** Many businesses and government organisations lack the necessary resources, expertise, and training to effectively defend against cybersecurity threats. This deficiency in technical capabilities puts personal data at risk and undermines data privacy measures.

---

<sup>30</sup> Dilip Modi, *Fostering digital literacy in rural India*, ETBFSI, Sep. 25, 2022, <https://bfsi.economictimes.indiatimes.com/blog/fostering-digital-literacy-in-rural-india/94402027>.

## **Digital Transactions And The Rise Of Cybercrimes: Testing The Readiness Of The Indian Legal Structure**

**3. Lack of technical expertise among law enforcement agencies:** One of the major challenges in India's cybercrime landscape is the lack of specialised knowledge and skills among law enforcement agencies. This deficiency hampers their ability to effectively investigate and prosecute cybercrime cases. As a result, there is a lack of accountability and deterrence for cybercriminals. It is crucial to provide comprehensive training and resources to law enforcement personnel to bridge this knowledge gap and enhance their capabilities in handling cybercrime. By doing so, the accountability of cybercriminals can be improved, leading to a stronger deterrent against cybercrime activities.

**4. Coordination challenges:** The lack of coordination among law enforcement agencies and government departments in India hinders the effective investigation and prosecution of cybercrime cases, particularly those that involve multiple jurisdictions. This coordination gap creates challenges in sharing information, collaborating, and allocating resources needed for successful investigations. As a result, it becomes challenging to gather evidence, apprehend cybercriminals, and ensure a swift legal process. Enhancing coordination mechanisms and establishing clear protocols for cross-jurisdictional cybercrime cases is crucial to overcome this hurdle and improve the efficiency of cybercrime investigations and prosecutions.

**5. Outdated cyber laws:** Existing cyber laws in India may lag behind the rapid pace of technological advancements and the ever-changing landscape of cybercrime. This creates difficulties in effectively prosecuting cybercriminals who use modern technologies. The Digital Personal Data Protection Bill of 2022 has faced criticism for certain provisions that privacy advocates argue could put personal data at risk due to their broad and ambiguous interpretation. Furthermore, Section 66A<sup>31</sup> of the IT Act was struck down by the Supreme Court of India in the case of *Shreya Singhal v. Union of India*<sup>32</sup> because it was deemed unconstitutional and violated the right to freedom of speech and expression. The court ruled that the provision allowed for arbitrary and excessive restrictions on online speech. Therefore, it is critical to upgrade existing laws to keep up with revolutions and the crimes that result from them.

---

<sup>31</sup> Information Technology Act, 2000, § 66A, No. 21, Acts of Parliament, 2000 (India).

<sup>32</sup> *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

**6. Challenges in e-Governance Implementation:** The National E-Governance Plan (NEGP) has faced significant challenges in its implementation, with many states struggling to provide the necessary infrastructure and resources. Although the Indian government is spending a lot of money on e-government projects, these projects are not successful in all parts of India. One of the main reasons for the same is the gap, or “digital divide”, that is prevailing in most parts of India. Not all regions in India are technologically equipped, which further raises the concern of an unequal distribution of ICT services.

**7. Slow legal process:** Insufficient workforce and subject-matter expertise within the legal system result in delays in the investigation and prosecution of cybercrime cases. These delays impede the accountability of cybercriminals and can discourage victims from reporting incidents. To tackle this issue, it is important to strengthen the legal and executive sectors by increasing the workforce and enhancing subject matter expertise.

Addressing these identified drawbacks and criticisms requires a collaborative effort involving the government, businesses, civil society, and law enforcement agencies. It entails raising awareness about data privacy rights and obligations, providing technical training and resources, improving coordination among relevant entities, updating cyber laws to align with technological advancements, bridging the digital divide, and enhancing the efficiency of the legal process. By addressing these inadequacies, India can better protect data privacy and effectively combat cybercrime.

## VII. POLICY RECOMMENDATIONS

Traditionally, the world had only witnessed physical or corporeal frauds and scams, and it can be seen that the world lacked the regulations and expertise necessary to tackle the sudden changes that the digital revolution had brought with it. The legal ramifications surrounding the digital economy should not be the cause of an increase in cybercrime; instead, they must protect the privacy and trust of digital users worldwide.

To address these challenges and mitigate the risks associated with cybercrime, strong security measures, regularly updating software and systems, educating users about cybersecurity best practices, and fostering a culture of security awareness need to be implemented. Furthermore,

## **Digital Transactions And The Rise Of Cybercrimes: Testing The Readiness Of The Indian Legal Structure**

collaboration between different stakeholders is essential to combating cybercrime effectively and promoting responsible digital behavior.

The user's negligence or ignorance is the starting point for any digital crime. As a result, those in charge of the internet must always be aware of internet hunters and take precautionary measures. The need to educate citizens who are reluctant to adopt such technological revolutions about IT and digital apps cannot be overstated. As it is said, *"The best way to save yourself from a hacker is to hack yourself."*

In the modern world, where hardly any home is without a smart device, it is essential to inculcate, in the curriculums of educational institutions, the measures to tackle cybercrimes to instil a culture of responsible digital behaviour from an early age by conducting regular awareness drives targeting organizations, businesses, and even remote areas, promoting cybersecurity education, etc. in order to uplift technological literacy.

The Indian cybersecurity laws have been amended several times since the IT Act was first enacted in 2000. Amendments often create ambiguity and a lack of uniformity. To maintain widely recognised cybersecurity standards, India must enact more holistic and informative cybersecurity legislation, as well as clarify regulatory requirements and make policy changes to develop a better cybersecurity structure and data protection laws. Applying a similar methodology to cyber security laws as that of environmental laws, with specific and distinct rules for different aspects, can be a plausible approach. Just as environmental laws address distinct areas such as air, land, and water, cyber security laws can be tailored to various aspects of the digital realm.

It is crucial to strengthen cybercrime laws by reviewing and updating existing legislation to address emerging threats. This involves clearly defining cybercrimes and establishing appropriate penalties that reflect the severity of the offenses. Additionally, fostering international cooperation and extradition treaties can facilitate cross-border investigations and prosecutions of cyber criminals.

Enhancing law enforcement capabilities is another vital aspect of curbing cybercrime. This includes investing in training programs for law enforcement personnel, equipping specialized cybercrime units with the necessary tools and technologies, and fostering collaboration between law enforcement agencies and the private sector.

Public-private partnerships play a significant role in implementing cybersecurity policies and legislation. The Cybersecurity Information Sharing Act, 2015<sup>33</sup> (CISA) allows government agencies and private entities to share information about cyber threats and defensive measures<sup>34</sup>. It aims to improve cybersecurity by facilitating information sharing across sectors and agencies. Governments should encourage collaboration between government agencies, private sector entities, and civil society organizations. By working together, they can develop coordinated strategies, share information and best practices, and undertake joint initiatives to strengthen cybersecurity measures across industries.

International cooperation is essential in the fight against cybercrimes, particularly in the case of transnational offenses. Governments should actively engage in international forums, such as INTERPOL and United Nations initiatives, to share intelligence, establish protocols for cooperation, and harmonise efforts to combat cyber threats globally.

It is all-important to create legislation that prevents financial fraud in light of advancements in the digital economic sector, such as blockchain technology and the growth of the e- investments market. Furthermore, better and more cost-effective online infrastructure for digital payment setups can be provided so that services are easily accessible to all segments of society. To deal with the globalised era of digitalization, it is critical for the Indian legal system to learn from its mistakes of the past and implement the recommendations that are feasible in approach. By examining the structures of digitally advanced economies, we can create better institutions for governance, offer a solid and stable system to an emerging nationlike India, and elevate the Indian fintech industry to a higher pedestal.

International jurisdictions have taken various approaches to tackle fintech fraud. To illustrate, key aspects of the GDPR include defining obligations for organizations to safeguard personal data and maintain privacy, granting individuals specific rights that can be legally enforced, and empowering regulators to demand proof of accountability and impose severe penalties for failure to comply. Additionally, it addresses jurisdictional conflicts that may arise when resolving international issues. As a result, continuous monitoring and adaptation to evolving fraud techniques are essential to ensuring the integrity and trustworthiness of the fintech ecosystem.

---

<sup>33</sup> Cybersecurity Information Sharing Act, 6 U.S.C § 754 (2015).

<sup>34</sup> The Federal Government of USA, Cyber Threat Indicators and Defensive Measures under the Cybersecurity Information Sharing Act of 2015, (Issued on February 16, 2016).

## **Digital Transactions And The Rise Of Cybercrimes: Testing The Readiness Of The Indian Legal Structure**

### **VIII. CONCLUSION**

With its ability to conduct business without regard to national boundaries and its significant impact on every sector of society, the digital economy continues to spur advancement not only in India but also all over the world. Although there are laws and statutes governing online activities, it is imperative to ensure that these rules keep up with the latest industrial advancements. In the upcoming years, we are expected to witness a plethora of initiatives that will contribute to evolving cyber legal frameworks and related ecosystems in India. One of the required developments in Indian cyber law jurisprudence is the National Cyber Security Strategy. This strategy not only aims to build on the National Cyber Security Policy but also serves as a thorough guiding principle for people, decision-makers, and other stakeholders. The plan shall shed more light on appropriate response mechanisms concerning the enhancement of the public sector and other industries. To address jurisdictional challenges, international cooperation and collaboration are crucial. Countries strengthening their legal frameworks, enhancing capabilities for investigating and prosecuting cybercrimes, and establishing mechanisms for swift and effective information sharing will improve coordination and standardisation of laws, and international agreements can help overcome these challenges and facilitate the global fight against cybercrimes. Only by identifying gaps in the digital economy and implementing targeted digital solutions can a complex regulatory system be resolved. If artificial intelligence is employed to commit cybercrime, then it can also contribute to the development of a powerful digital force within the legal system. As a result, it is possible to conclude that India, as one of the top scorers in digital thrift, can also have solid legal structures, but only if legislation is enacted without any ambiguity or obfuscation to ensure the utmost protection of digital users' personal data.