

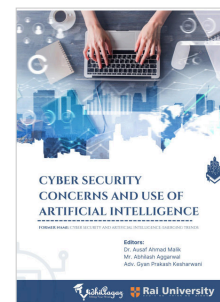
CHAPTER 1

Legal Challenges in Cross-Border Data Transfers amid Financial Cyber Crimes

Nandini Braj Singh and Disha Singhal

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 1–14

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Nandini Braj Singh & Disha Singhal, *Legal Challenges in Cross-Border Data Transfers amid Financial Cyber Crimes*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 1 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Nandini Braj Singh and Disha Singhal, 'Legal Challenges in Cross-Border Data Transfers amid Financial Cyber Crimes' in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 1.

CHICAGO (17TH ED.)

Singh, Nandini Braj, and Disha Singhal. "Legal Challenges in Cross-Border Data Transfers amid Financial Cyber Crimes." In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 1–14. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-1/>.

APA (7TH ED.)

Singh, N. B., & Singhal, D. (2024). Legal challenges in cross-border data transfers amid financial cyber crimes. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 1–14). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-1/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-1/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

LEGAL CHALLENGES IN CROSS-BORDER DATA TRANSFERS AMID FINANCIAL CYBER CRIMES

Nandini Braj Singh¹ and Disha Singhal²

ABSTRACT

This paper, under the theme "Law Enforcement and Procedural Challenges: Data Protection Norms and Challenges in Fraud Detection" with the title "Legal Challenges in Cross-Border Payments Amid Financial Cyber Crimes", critically delves into the intricacies of cross-border data transfer regulations with respect to rising financial cybercrimes. Global interconnectedness introduces considerable challenges to data protection and security, giving rise to legal ambiguities that cybercriminals exploit. For that reason, this paper shall also evaluate the impact of data transfer on the global digital economy. This paper presents a pre-requisite description of the evolution of cybercrimes in the financial domain, starting from traditional fraud to sophisticated cyberattacks, showcasing the increasing complexity of financial crimes and regulatory bodies' subsequent difficulties in promptly addressing these issues. This study will also cater to a comparative analysis between global regulatory frameworks and India's recent legislation, Digital Personal Data Protection Act (DPDPA) 2023, to identify potential gaps in protecting financial personal identifiable information and evaluate the effectiveness of existing data protection measures in addressing cyber-oriented financial crimes and to propose potential solutions. Consequently, this paper shall provide a detailed strategy for the mitigation of financial cybercrimes in a twofold manner: Technological Solutions, such as encryption, blockchain, and multi-factor authentication; and Organizational Practices, such as Risk Management and Incident Response Planning. Further, exploring financial cybercrimes through the lens of feminist jurisprudence, this study also aims to understand whether women are equipped with coherent abilities to deal with financial cybercrimes through empirical research, employing methodologies such as questionnaires and case studies along with a narrative review. Therefore, by examining real-world case scenarios and gathering data on individual experiences, this research seeks to connect theoretical frameworks with present executive practices.

Keywords: Cross Border Data Transfer, Cyber Financial Crimes, Sensitive Personal Data, Digital Economy, Digital Personal Data Protection, Strategy, Global Impact.

INTRODUCTION

In the interconnected world of the 21st century, cyberspace has become a platform with no tangible boundaries that binds societies from different parts of the globe together. Through this medium, information flows seamlessly across borders, transforming the traditional boundaries of communication and commerce (What Is Cross-Border Data Transfer?, n.d.). A 2020 Organization for Economic Cooperation and Development (hereinafter referred to as OECD) Report confirmed that cross-border data transfers have increased local wages and drawn greater investments in local infrastructure, thereby improving national economies and helping developing countries integrate into the global economy (Returns to Intangible Capital in Global Value Chains, 2020). Due to the prevalence of and easy access to cyberspace, cybercrimes have become an unintended consequence. The inherent greed of humans and the dependence on technology have made society vulnerable to cybercrimes of various kinds. The

¹ Student at Symbiosis Law School, NOIDA, India.

² Student at Symbiosis Law School, NOIDA, India.

digitalization of economies has paved paths for cybercriminals to gain illegal benefits by committing cyber-financial crimes. Cyber-financial crimes are illegal activities that are done through the medium of computers to gain some financial gain. Transnational cyber-financial crimes have become a significant risk to the global financial system's stability (Meda, 2024). Cybercriminals have found their way to abuse loopholes in the financial infrastructure, such as weak and insufficient cybersecurity frameworks, and commit fraudulent financial transactions internationally.

Cyber fraud is an umbrella that encompasses various kinds of financial crimes aimed at threatening the privacy and security of individuals as well as business entities to cause them financial losses. These include identity theft, phishing, malware attacks, and cyber-attacks on financial institutions and any criminal activity targeting financial entities and markets (Syaufi, 2023, p. 87). The advancement in e-banking and technology has accelerated the growth of cyber-financial crimes. Identity theft, one of the most heinous methods, refers to the attacker's theft of an individual's identity to use it to fraudulently take over financial accounts, like credit cards and bank accounts, to commit cyber fraud. Moreover, with the help of Artificial Intelligence, it has become easier to tailor synthetic media, called deepfakes, that further paves the way for criminals to manipulate the victim and perpetrate identity theft (Meda, 2024). In addition to causing financial loss to the victim, this also promotes the funding of unlawful activities such as money laundering and terrorism by supporting the cross-border movement of illicit funds (Syaufi, 2023, p. 87).

LEGAL FRAMEWORKS FOR REGULATING CROSS-BORDER DATA TRANSFERS

With the rising prevalence of cross-border data transfers globally, various countries have recognised the need to regulate these transfers to safeguard their citizens and industries from such financial attacks. The United States' Fair Information Practice Principles (FIPP), formulated in the 1970s, is the root of data protection principles. The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 1980 are based on accountability, minimization, quality and integrity, purpose specification and use limitation, transparency, security safeguards, openness and individual participation. Even the provisions of the General Data Protection Regulation of the European Union can be traced back to the Guidelines (Sun, 2023, 172-173).

ENSURING COMPLIANCE WITH THE GDPR

The EU's General Data Protection Regulation (hereinafter referred to as GDPR) prohibits transfers outside the EU unless the recipient country provides an equivalent level of protection. An adequacy decision is made, which involves investigating the data protection standards of the recipient country on a case-to-case basis by the EU. Once granted, an adequacy decision removes restrictions on data transfers to that country (General Data Protection Regulation (GDPR), 2016, Article 45). If a country is not covered under an adequacy decision, Article 46 of the GDPR enlists transfer tools that provide appropriate safeguards for the transfers (General Data Protection Regulation (GDPR), 2016, Article 46). They are:

- Standard Contractual Clauses- These are standardized contracts that ensure appropriate safeguards for data protection (General Data Protection Regulation (GDPR), 2016, Article 46(2)(c)).
- Binding Corporate Rules- These rules are generally adopted by companies that deal with many data transfers to ensure adequate data protection (General Data Protection Regulation (GDPR), 2016, Article 47).
- Code of Conduct- This is a set of binding rules adopted by an organization to demonstrate compliance with the GDPR. Such codes are prepared by industry representatives and are pre-approved by the data protection authorities.
- Certification- This enables data transfers to organizations that have received certification from the authority or European Economic Areas Data Protection Authorities.
- Ad Hoc Contractual Clauses- In case the data controllers or processors don't use the SCCs, they can opt for ad hoc contractual clauses that the national Data Protection Authority must pre-authorize.

Other than this, transfers can also be made utilizing Article 49, which provides derogations for specific situations, such as explicit consent, contractual performance, public interest, establishment, exercise or defence of legal claims, protection of interests of a data subject incapable of giving consent, or to provide information to the public. A necessity test is required to determine the necessity of transferring personal data for derogation, for derogation is not a rule but only an exception.

WHAT DOES DPDP HAVE TO SAY ABOUT CROSS-BORDER DATA TRANSFERS?

The Digital Personal Data Protection Act (hereinafter referred to as DPDPA) in 2023 balances the right of individuals to protect their personal data and the need to process such personal data for lawful purposes (Digital Data Protection Act, 2023, (NO. 22 OF 2023)). It addresses several concerns relating to privacy, national security, and cross-border data flow. Section 16 enables the transfer of the personal data of the Data Principal by the Data Fiduciary to all countries except for those notified by the Central Government (Digital Data Protection Act, 2023, (NO. 22 OF 2023), s.16(1)). It also goes on to state that if any existing law provides for more stringent protection or restriction on transferring personal data outside India, then those provisions shall prevail over the Act (Digital Data Protection Act, 2023, (NO. 22 OF 2023), s.16(2)). This means even if the Government allows the transfer of personal data to a specific country but under sectoral laws, such transfer is prohibited for data localization purposes, then the transfer shall not be permissible. For instance, under the Payments and Settlements Act, 2007, the Reserve Bank of India has directed to localize data regarding the digital payments sector (The Payments and Settlements Act, 2007 (Act no. 51 of 2007)). With this, the Indian authorities can track suspicious transactions and have quicker access to such data when investigating fraud. This also allows for greater transparency in the cross-border payments system. It also limits the ability of fraudsters to exploit regulatory gaps in other jurisdictions (Srivastava, n.d.).

Further, Section 17(1) lays down certain exemptions as to when cross-border transfers cannot be restrained in any case, such as when the processing of personal data is necessary for enforcing a certain legal right; for the performance of any judicial, quasi-judicial, regulatory or supervisory function; prevention, detection, investigation or prosecution of any offence or contravention of any law; pursuant to any contract entered; for a scheme of compromise or arrangement or merger or amalgamation of two or more companies; and to ascertain the finances of a defaulter to a financial institution (Digital Data Protection Act, 2023, (NO. 22 OF 2023),s.17(1)). The Act is also extra-territorially applicable, i.e. if any foreign entity collects personal data from India, they shall be subjected to the provisions of the Act and mandated to comply with them. However, it is pertinent to note that the Central Government has yet to come up with rules and regulations for the Act and its implementation, and only with those rules shall the application of the Act be clear.

LEGAL CHALLENGES IN CROSS-BORDER PAYMENTS

With the increase in globalisation and e-commerce, cross-border payments require multiple intermediaries on both sides, such as commercial banks, money service businesses and fintech firms, and international and domestic payment systems. Broadly, cross-border transactions involve two types of intermediaries: a front-end intermediary that interfaces with an end user and a back-end intermediary for exchanging and settling funds (Stuck in the Middle: Observations From Intermediaries in Cross-Border Payments for CBDC Design, 2021). These front-end intermediaries, such as commercial banks or other payment service providers (PSPs), depend mainly on the back-end intermediaries, such as neobanks and money transfer operators, for the transaction (Ibitola, 2023). Back-end intermediaries operate through several models, broadly classified as correspondent banking, interlinking of payment infrastructures, closed-loop, and peer-to-peer.

The role of intermediaries in cross border payments arose out of necessity to complete the steps after the user has made a command to complete a transaction, these steps help in completing the components of the transaction, making it reach the targeted location/user, therefore, forming a transaction chain. It is observed that when intermediaries have outsourced their operations to third party providers, especially for checking KYC and AML protocols have often created a loophole in this chain, thereby increasing the risk of fraud (Stuck in the Middle: Observations From Intermediaries in Cross-Border Payments for CBDC Design, 2021).

These intermediaries communicate through SWIFT messages as a security measure and to fastrack this complex transaction process. SWIFT, even after being a highly secured network, depends on the credibility of its participants for its security (There Is No Alternative: SWIFT as Infrastructure Intermediary in Global Financial Markets, 2019). Participants who are weak in terms of following their cybersecurity measures, lead a pathway for cyber criminals to use the transaction chain they are working on, to commit financial fraud (NELSON, n.d.). When working through a centralised system, which requires a large amount of intermediaries, layers are built, increasing the complexity of the chain, hence, making the origin of the transaction, harder to trace. This challenge arises due to the fragmentation of the information among intermediaries across jurisdictions (Meli & Baer, 2023).

Unauthorized SWIFT messages through compromised intermediary banks in the transaction change is yet another challenge for cross-border transactions, as this approach is often used to hack their systems, send fraudulent messages through these compromised systems and further instructing the transfer of funds to illegitimate accounts, increasing the risk for fraud and money laundering (How Banks Are Combating Cyber Attacks on Their SWIFT Payments, n.d.). The Bangladesh heist in 2016, is a key example of how vulnerabilities in an intermediary institution's security can lead to a large-scale fraud. This heist was successful using fraudulent messages sent via SWIFT, leading to a loss of \$81 million (Bangladesh Hack Illustrates Rising Sophistication of Attacks, n.d.).

JURISDICTIONAL CHALLENGES

Jurisdictional challenges are exacerbated in cybercrime cases, especially in cross-border payments, because perpetrators often operate across multiple borders, and their attacks may be launched from jurisdictions that do not cooperate with international investigations. Fraudsters frequently exploit jurisdictions with weak or non-existent cybercrime laws, like countries with low AML and KYC compliances, which includes Iran and Monaco etc. or lenient regulation over the SWIFT network, like Lebanon and Panama, to target financial institutions in other countries. This methodology is often referred to as Regulatory arbitrage (High-Risk Third Countries for AML Purposes, n.d.).

This challenge further increases with the current adaptation towards DLT-like Blockchains, which reduces the need for centralized intermediaries in the transaction process but as being a developing and innovative solution, many countries are yet to decide on their regulations (MORGAN, n.d.). With the increase in the use of digital assets, cryptocurrencies, and decentralized finance (DeFi), regulatory arbitrage is becoming common when users leverage jurisdictions with relaxed rules on these emerging technologies to conduct illegal transactions, including fraud, with relative anonymity (Recommendations for Regulating and Supervising Bank and Non-Bank Payment Service Providers Offering Cross-Border Payment Service, n.d.).

Regulatory arbitrage has led to two major developments in Fraud:

- 1) Fraud through Layering and Obfuscation: Regulatory arbitrage is often used by fraudsters to complex the structures in the transaction process, which disrupts the origin of the transaction for example, if a fund is being transferred from one place to another, the place of origin of the funds may never be traced due to such high complexities inserted in the channel. This makes tracing & auditing transactions difficult (The 3 AML Stages: Layering, Placement, & Integration Explained - Blog, 2024).
- 2) Fraud via Jurisdiction Shopping: Often hiding behind shell companies, Fraudsters participate in business transactions between jurisdictions with lenient laws for payment systems and further registration procedures, choosing jurisdictions freely to transfer or steal money from once they set up their bases at a weaker regulated place (Illicit Financial Flows From Cyber-Enabled Fraud, n.d.).

MITIGATION STRATEGIES

Long Transaction Chains and involvement of intermediaries raised concerns all across the world. They led to the development of the SWIFT network with additional features and DLT Technologies as described below:

Mitigation Efforts Through SWIFT:

End-to-End Payment Tracking (SWIFT gpi): SWIFT gpi improves transparency and real-time tracking, providing better oversight of transactions as they move through intermediaries (Delivering Added-Value, n.d.).

Customer Security Programme (CSP): SWIFT's CSP requires participating institutions (including intermediaries) to strengthen their cybersecurity posture, mitigating the risk of fraud through hacking or unauthorized access to SWIFT systems (Customer Security Programme (CSP), n.d.).

Fraud Detection Tools: SWIFT also provides tools like Sanctions Screening and Payments Data Quality services that help financial institutions, including intermediaries, detect and prevent illicit transactions that may be part of fraudulent schemes (Swift and Global Banks Launch AI Pilots to Tackle Cross-Border Payments Fraud, 2024).

KYC and AML

KYC is a process for verifying individuals before they participate in any sort of cross-border payments, whereas AML regulations help in monitoring payment patterns that are suspicious, both helping in the early detection of fraudulent transactions like money laundering.

Multi-Factor Authentication

MFA is a security feature that scales up protection efforts by mandating that users provide two or more verification methods. For instance, a combination of a passcode and mobile identity is one of the most potent tools applications can use to make it hard for hackers to enter financial systems. It adds another layer of security which ensures that any kind of unauthorised access is prevented even if one security factor (like a password) is compromised without the second authentication factor.

Real-time monitoring and AI-based fraud detection

AI-based security has been proven to be fruitful, especially in identifying abnormalities in patterns of transactions that may be risky, which may include large transfers to unfamiliar accounts, sudden spikes in activity, or transfers to high-risk jurisdictions(Tennant, n.d.).

AI-based security systems even send real-time notifications to the transactors, which prevents any damage to sensitive financial data and provides fast and secure cross-border transactions. Real-time monitoring using AI and training these machines using historically collected data allows for the immediate flagging and halting of suspicious transactions, preventing fraudulent activities from being completed.

D.L.T.

Distributed Ledger Technology is a system that is decentralised in nature, where transaction participants

have access to the same records in a synchronised manner, maintaining transactions in a secured channel protected by cryptography(GAO-19-704SP, Science & Technology Spotlight: Blockchain & Distributed Ledger Technologies, n.d.). This reduces the need for intermediaries and mitigates any security risks they pose. One of DLT's main features is immutability, as once data is stored in this decentralised mechanism, it is hard to alter such data(World Bank Document, n.d.). There are various types of DLT, but one of the emerging ones is blockchain.

Blockchain Technology

Blockchain is a technology which, instead of sending data collectively in a centralized manner across the transaction chain requiring multiple intermediaries to receive it, only records transactions in a decentralised manner in smaller units called “blocks” connected in “chain” like channel across multiple locations each time in a unique pattern, This makes the procedure of sending and receiving money easy and quick. This process, being decentralised, also does not require intermediaries in the transaction chain; therefore, it is considered a user-friendly and peer-to-peer transfer (How DLT, APIs, and CBDCs Are Changing Cross-Border Payments, 2024). Blockchain technology helps increase transparency and security in cross-border transactions. This is because each transaction is recorded and sent across in a unique manner, which is difficult to alter without the consensus of the network. Such unique and secure transactions, which are also easily traced, further aid in detecting fraudulent activities before any major losses like money laundering or cyber terrorism.

Encryption

Encryption, if understood from an analogy, puts our sensitive data under a lock as soon as we transmit it, allowing only the one to whom it is sent, with a key, can decrypt it, which means that until the target is reached, no one can access the information in the transaction channel. For cross-border payments, encryption locks away all the sensitive information of the payer, making the transaction secure compared to other means, which reduces the risk of fraudulent activities in the transaction channel.

Risk Management in Cross-Border Payment Frauds

Organisations in the current digital era often invest in a dedicated and independent Fraud Control unit equipped with professionals with experience in fraud detection and risk management using mitigation strategies discussed above in this paper. Industries Today, while providing training to their employees for their respective fields, ensure that risk management training becomes a part of it, which helps develop precautionary measures for financial fraud. It is suggested to organisations that cybersecurity professionals undertake risk assessments to address any vulnerabilities that may arise in multiple transactions exercised by firms every day. Moreover, Proactive measures such as fraud simulation testing and advanced analytics integrated with machine learning can help detect weaknesses in the present infrastructure of the organisation (Combating Fraud in the Era of Digital Payments, n.d.).

Incident Response Planning in Cross-Border Payment Frauds

Incident Response Planning is a matter of internal grievance redressal mechanism of an organisation,

which is generally dealt with by the Fraud Control unit by experts in fraud cases and cybersecurity. Incident response planning is constantly upgraded as per the emerging technologies, such as the shift to blockchains, the preparation for risks attached to it, and timely reports to senior management to critically evaluate the organisation's preparedness to detect fraudulent activities. Customer awareness programs are vital apart from building a response team to educate customers on the risk of digital transactions and safety protocols. Adding to this, the setting up of mechanisms and detailed procedures helps in the quick detection of fraud. Currently developed technologies like resistance AI work at an advanced level, ensuring real-time monitoring and checking the legitimacy of the devices. At the same time, regulatory frameworks guide the compliance efforts of financial institutions (FIs)(Combating Fraud in the Era of Digital Payments, n.d.).

CASE STUDY

To discuss how societal structures of gendered roles and financial independence interlink with the vulnerabilities of women to financial cybercrimes, the authors have conducted a survey in a sample size of 100 women.

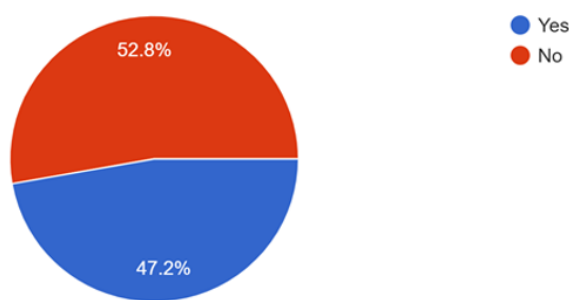


Figure 1. Have you ever received financial literacy training (formal or informal)?

Survey results suggest that even after 47.2% of women have received financial literacy training, they are more susceptible to financial cybercrime largely due to lower financial independence and lack of awareness. Financial independence, in this context, is not an individual matter but rather a function of broader social, economic, and legal infrastructure.

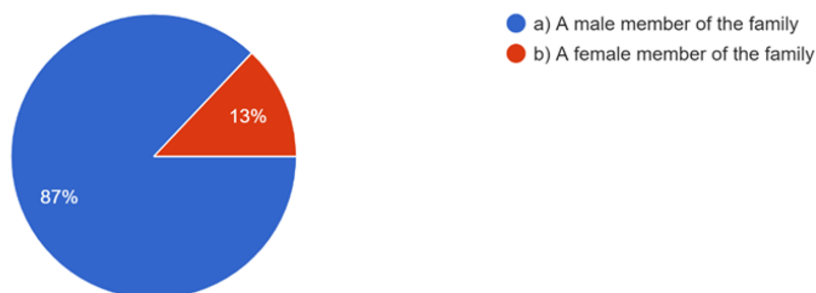


Figure 2. If you have been a victim to cyber financial crimes, who do you go to seek first-hand advice from?

Interestingly, the study finds that 87% of female victims consult their male family members for advice because they feel men are better placed to understand the transactions, hence reinstating the stereotypical gender roles that restrict the right of women to act independently in financial affairs. Legal systems must first work to rebalance these power dynamics by providing equal access to financial tools and helping an environment where women feel empowered to make independent decisions over their finances in order to arm women with coherent abilities to deal with financial cybercrimes. That includes not only financial literacy but also some tearing off of societal expectations that would discourage women from really engaging intimately with financial systems. The two salient reasons for women's over-exposure to financial cybercrimes that the survey fetches are unfamiliarity and scams targeted at the gender. This follows from the systemic exclusion of women from platforms where financial education and decision-making are conducted. In most societies, women remain without equal access to financial literacy programs. This lack provides a gap between their preparedness to handle financial risks across genders. Suggestions, made by some of the participants themselves, include awareness programs for cybersecurity and financial independence so that they build confidence in handling their finances and be less susceptible to such frauds. Thus, based on this survey, it can be determined that women are educated and formally trained. However, societal norms and economic inequalities hold them back as coherent abilities to deal with financial cybercrimes. Women's Empowerment in this space must come through legal reforms and cultural changes toward true gender equality in financial autonomy and cybersecurity.

CRITICISM OF THE DPDPA

Following the 2017 judgement of Justice K.S. Puttaswamy and Anr. v. Union of India and Ors., where the right to privacy was recognised as a fundamental right, the government constituted a committee chaired by Justice B N Krishna to recommend a proper legal framework for data protection (Greenleaf, 2018). The Committee, in its report, recommended forbidding cross-border transfers of sensitive personal data due to historically unregulated transfers leading to violation of privacy and unlawful processing (Srivastava, n.d.). It is intriguing to note that initial drafts of the DPDPA distinguished between critical and sensitive personal data, but the same cannot be found in the DPDPA. This distinction was essential for data protection and localization. However, now it may be on the discretionary power of the Government to notify on a case-to-case basis (India: Digital Personal Data Protection Act, 2023 - What It Means for Cross-Border Transfers, 2023). The Act is also silent on further transfers of data, therefore, creating a vacuum, i.e. a company belonging to a blacklisted country may obtain data from a company belonging to a non-blacklisted company.

With respect to Section 16 (1), the Act does not specify the grounds for restricting the transfer of personal data to a country notified by the Government (Digital Data Protection Act, 2023, (NO. 22 OF 2023),s.16(1)). The Act does not prescribe any adequacy check or security requirements that the Data Recipients and Data Fiduciaries should maintain, nor any adequate safeguard agreement format to execute with the Data Recipients to process the data. Moreover, it is not clear whether or not Data Recipients will be notified by the government if their laws are appropriate or not for such transfers. It may be clearer once the government releases the rules for DPDPA, which will detail the adequacy

checks that need to be carried out for cross-border data transfers (Srivastava, n.d.). The provisions of the Act on the restriction of data transfers lack specificity and clarity, which may expose an individual's personal data when it is being sent to countries with significantly weaker data protection laws. It has been further argued that the Data Protection Board may not be independent and effective due to its short-term appointments, which may portend bias or even external influences.

RECOMMENDATIONS

Considering the overall research in this paper, the following recommendations are proposed:

- Criteria for evaluating countries have to be made strict and detailed with standards that protect the personal data of Indian citizens effectively, apart from the cross-border transaction data that is regulated by RBI.
- Real-time fraud detection systems, both as precautionary measures and cyber forensic tools, have helped in mitigating fraud with their constant development of machine learning and Artificial Intelligence for monitoring suspicious transactions; if applied uniformly globally, along with systems like SWIFT, Fraud detection can become much simpler and easier in the future days.
- Conducting risk assessments at periodic intervals is necessary, and providing a report to the Data Protection Board would bring accountability in protecting data leaks and further help in understanding areas where data is more vulnerable to leaks.
- Introduce an adequacy decision mechanism similar to GDPR, which allows transfers to countries with adequate levels of data protection. This system can ensure that personal data transferred outside India will be treated with similar safeguards. India needs inspiration from an adequacy decision mechanism similar to GDPR, which permits transfers to countries with a high-security standard for data protection. This mechanism will ensure that the personal data of Indian citizens transferred outside India will be treated with similar precautions.
- India, being a highly populated country, must work towards building a risk-based approach similar to Singapore's PDPA, which has clear demarcation for the transfer of data based on the amount of risk posed by the receiving country.
- An amendment can be made to the DPDPA of India to insert a certification mechanism specifically for data fiduciaries and other cross service providers who process sensitive data involved in cross-border payments.
- Maintenance of an audit trail for cross border transactions in each organisation for keeping a verified record of data transfer, shall be made accessible to for investigations to inquire for cases of fraud and other cyber security breaches by amendment as a mandate under Section 16 of the DPDPA.

CONCLUSION

After thoroughly analyzing all the literature, we conclude that financial cybercrimes require keen attention at both national and international levels, where countries need to strengthen their cyber security laws to reduce fraudulent activities in their jurisdiction. Concerning India, though DPDPA has

been proven to be fruitful for a blanket Data Protection outlook, it still requires amendments to deal with cross-border data transmission in the complete sense, including cross-border payments, which may not come easy as they must comply with the PMLA and RBI's directives for cross border payments. Regulatory Arbitration has been seen as a big issue that requires uniform global attention with treaties and the implementation of cross-border regulations to prevent fraudulent activities. The boom in technology like blockchain encryption and AI also serves in the best interest of the cyber security and cyber Forensic dimensions to mitigate fraud efficiently.

While the above is catered to, it is also vital to keep a check on making such strategies gender sensitive as the case study submitted in this paper suggests that women feel underconfident to tackle financial cybercrimes independently while some suggest that they prefer or trust a male member of the family to deal with such risks or circumstances with reasoning that they are more qualified to deal with the same, creating a strong need for increasing financial security literacy for women for them to be truly independent which will be supported by government initiatives and gender sensitive approach towards the policies and laws making them accessible for all.

REFERENCES

1. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. OJ L 119, 4.5.2016, p.Art. 45 GDPR – Transfers on the basis of an adequacy decision - General Data Protection Regulation (GDPR)
2. Digital Personal Data Protection Act (DPDP Act), No. 22 of 2023, India Code (2023). https://www.indiacode.nic.in/bitstream/123456789/24073/1/dpdp_act_2023.pdf
3. The Payments and Settlements Act, 2007(Act no. 51 of 2007) <https://www.indiacode.nic.in/bitstream/123456789/2082/4/a2007-51.pdf>
4. The 3 AML Stages: Layering, Placement, & Integration Explained - Blog. (2024, May 16). Unit21. Retrieved October 23, 2024, from <https://www.unit21.ai/blog/3-stages-of-money-laundering-placement-layering-integration>
5. Bangladesh hack illustrates rising sophistication of attacks. (n.d.). KPMG. Retrieved October 23, 2024, from <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2016/08/swift-it.pdf>
6. Combating fraud in the era of digital payments. (n.d.). PwC India. Retrieved October 23, 2024, from <https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/combating-fraud-in-the-era-of-digital-payments.pdf>
7. Customer Security Programme (CSP). (n.d.). Swift. Retrieved October 23, 2024, from <https://www.swift.com/myswift/customer-security-programme-csp>
8. Delivering added-value. (n.d.). Swift. Retrieved October 23, 2024, from <https://www.swift.com/our-solutions/swift-gpi/swift-gpi-banks/delivering-added-value>

9. GAO-19-704SP, Science & Technology Spotlight: Blockchain & Distributed Ledger Technologies. (n.d.). Government Accountability Office. Retrieved October 23, 2024, from <https://www.gao.gov/assets/gao-19-704sp.pdf>
10. Greenleaf, G. (2018, July 27). A Free and Fair Digital Economy Protecting Privacy, Empowering Indians Committee of Experts under the Chairmanship of Justice B. MeitY. Retrieved October 23, 2024, from https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
11. High-risk third countries for AML purposes. (n.d.). The Law Society. Retrieved October 23, 2024, from <https://www.lawsociety.org.uk/topics/anti-money-laundering/high-risk-third-countries-for-aml-purposes>
12. How Banks are Combating Cyber Attacks on Their SWIFT Payments. (n.d.). Eastnets. Retrieved October 23, 2024, from <https://www.eastnets.com/white-papers/how-banks-are-combating-cyber-attacks-on-their-swift-payments>
13. How DLT, APIs, and CBDCs are Changing Cross-Border Payments. (2024, May 6). Opus Technologies. Retrieved October 23, 2024, from <https://opustechglobal.com/how-dlt-apis-and-cbdc-are-changing-cross-border-payments/>
14. Ibitola, J. (2023, April 18). Preventing and Stopping Fraud in Cross-Border Payments. Flagright. Retrieved October 23, 2024, from <https://www.flagright.com/post/preventing-and-stopping-fraud-in-cross-border-payments>
15. Illicit Financial Flows from Cyber-Enabled Fraud. (n.d.). FATF. Retrieved October 23, 2024, from <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf>
16. India: Digital Personal Data Protection Act, 2023 - what it means for cross-border transfers. (2023, November 02). Onetrust Data Guidance. <https://www.dataguidance.com/opinion/india-digital-personal-data-protection-act-2023-what>
17. Meda, K. (2024, May 3). Identity theft is being fueled by AI & cyber-attacks. Thomson Reuters. Retrieved October 23, 2024, from <https://www.thomsonreuters.com/en-us/posts/government/identity-theft-drivers/>
18. Meda, K. (2024, May 3). Identity theft is being fueled by AI & cyber-attacks. Thomson Reuters. Retrieved October 23, 2024, from <https://www.thomsonreuters.com/en-us/posts/government/identity-theft-drivers/>
19. Meli, M., & Baer, J. (2023, March 31). Unmasking the hidden dangers: How cyber threats target intermediaries. Julius Baer. Retrieved October 23, 2024, from <https://www.juliusbaer.com/en/business-navigator/technology/unmasking-the-hidden-dangers-how-cyber-threats-target-intermediaries/>
20. Meltzer, J. P., Qureshi, Z., & Jeong, D. (2018, March 20). Regulating for a digital economy: Understanding the importance of cross-border data flows in Asia. Brookings Institution.

Retrieved October 24, 2024, from <https://www.brookings.edu/articles/regulating-for-a-digital-economy-understanding-the-importance-of-cross-border-data-flows-in-asia/>

21. MORGAN, J. (n.d.). Cross-border payment modernization. J.P. Morgan. Retrieved October 23, 2024, from <https://www.jpmorgan.com/payments/payments-unbound/volume-3/cross-border-payment-modernization>
22. NELSON, A. (n.d.). The Global Cyber Threat to Financial Systems – IMF F&D. International Monetary Fund (IMF). Retrieved October 23, 2024, from <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>
23. The Payments and Settlements Act. (2007). Universal.
24. Recommendations for Regulating and Supervising Bank and Non-bank Payment Service Providers Offering Cross-border Payment Service. (n.d.). Financial Stability Board. Retrieved October 23, 2024, from <https://www.fsb.org/uploads/BAFT.pdf>
25. Returns to intangible capital in global value chains. (2020, September 30). OECD iLibrary. Retrieved October 24, 2024, from https://www.oecd-ilibrary.org/trade/returns-to-intangible-capital-in-global-value-chains_4cd06f19-en
26. Srivastava, S. (n.d.). India: Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with GDPR and PIPL. Indian Journal of Law and Technology. <https://www.ijlt.in/search-results?q=India%3A+Decrypting+critical+concepts+under+India%27s+Digital+Personal+Data+Protection+Act%2C+2023+and+com>
27. Stuck in the Middle: Observations from intermediaries in cross-border payments for CBDC design. (2021, August 1). Bank for International Settlements. Retrieved October 24, 2024, from https://www.bis.org/events/cpmi_ptfop/proceedings/paper11.pdf
28. Sun, L. (2023, November). Overview of Regulations on Cross Border Data Flow. Academic Journal of Science and Technology, 8, 172-173. https://www.researchgate.net/publication/375855814_Overview_of_Regulations_on_Cross_Border_Data_Flow
29. Swift and global banks launch AI pilots to tackle cross-border payments fraud. (2024, May 30). Swift. Retrieved October 23, 2024, from <https://www.swift.com/news-events/press-releases/swift-and-global-banks-launch-ai-pilots-tackle-cross-border-payments-fraud>
30. Syaafi, A. (2023, June). Employing Forensic Techniques in Proving and Prosecuting Cross-border Cyber-financial Crimes. International Journal of Cyber Criminology, 17(1), 87. <https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/150/55>
31. Tennant, F. (n.d.). Cross-border payments: fraud mitigation strategies — Financier Worldwide. Financier Worldwide. Retrieved October 23, 2024, from <https://www.financierworldwide.com/cross-border-payments-fraud-mitigation-strategies>

32. There is no Alternative: SWIFT as Infrastructure Intermediary in Global Financial Markets. (2019, January 21). FinGeo. Retrieved October 23, 2024, from <https://www.fingeo.net/swift-as-infrastructure-intermediary-in-global-financial-markets/>
33. What is Cross Border Data Transfer? (n.d.). Securiti.ai. Retrieved October 23, 2024, from <https://securiti.ai/glossary/cross-border-data-transfer/>
34. World Bank Document. (n.d.). World Bank Document. Retrieved October 23, 2024, from <https://openknowledge.worldbank.org/server/api/core/bitstreams/5166f335-35db-57d7-9c7e-110f7d018f79/content>
