

Digital Disruption: In the Perspective of DPDP Act

Sandhya Bhandary S

Assistant Professor
Manjunatha Pai Memorial Government
First Grade College
Karkala
ssbhandary25@gmail.com

Anjali Ganesh

Professor
Department of Business Administration
St. Joseph Engineering College
Mangalore
anjali@sjec.ac.in

Abstract

The fintech industry in India has been growing exponentially and ranks as third-largest digital economy in the world. The impetus from the government towards a cashless economy, demonetization and the pandemic have been contributing factors for the digital push. The digital landscape in India is dynamic, characterized by a proliferation of businesses and startups offering technology-based financial services. These businesses have partnered with the regular financial service providers and to enhance the delivery of financial services through technological support. The surge in the number of fintech service has raised concerns of cyber security, data privacy, and the regulatory measures. Large volume of transactions in the digital payments, swelling of the cryptocurrencies beyond the governance of regulatory bodies, the contemplation of the RBI to usher digital currency to counter the cryptocurrencies assert the need for robust laws in the fintech sector. Customers have enthusiastically embraced the ease of doorstep one-click services and responded positively to technological advancements. Though the fintech industry is operating at Industry 4.0, the governing rules and regulations are in the early phase of guidelines and regulatory compliances. The multiple overlapping jurisdictions aggravate the challenges of the digital advancement.

Fintech being the intersection of finance and technology, remains largely unregulated. Digital economy in India has been vulnerable to cyber-attacks, frauds, data privacy and cross-border exchange of the customer information. Although, RBI, SEBI, IRDAI, TRAI have issued guidelines in their respective jurisdictions, they are insufficient to govern the rapidly evolving digital business models. The lack of clear jurisdiction boundaries and absence of exclusive laws in the digital economy to hold companies accountable has been one of the

regulatory concerns. The implementation of Digital Personal Data Protection Act, 2023 is one step in the direction of protecting the customer interest and rights.

This research paper examines the impact of the Digital Personal Data Protection Act on the evolving digital landscape. It aims to analyze the depth / profundity of the DPDP Act, its comprehensive coverage of digital activities, protection of digital data, mitigation of digital issues, and its role in reshaping digital governance. The study's findings will highlight the dynamic nature of digital business models, identify gaps between the operational digital economy and governance frameworks, and assess the DPDP Act's role as a stepping stone in digital governance.

Keywords: *Fintech, digital payment, digital currency, data privacy, digital economy*

Introduction

Technology is rapidly advancing and invading the conventional businesses. Today, the modern business houses use technology to enhance the operational efficiency, minimize costs and provide an enriching experience to its customers. The utility of technology and the benefits derived by both the business houses and customers is evident prominently in service sectors like financial services including banks, insurance, finance, mutual funds, hospitality, health and alike.

The traditional businesses predominantly in the financial sector are in the advantageous position with the implementation of technology thereby enabling them to deliver better service. The quick acceptance of the technology by the firms and customers led to massive change in the financial landscape, thus boosting the fintech revolution.

Objective

The objective of the research study is:

To analyse the provisions of the Digital Personal Data Protection Act and its applicability in the fintech context

To gauge the coverage of the Act with regard to the fintech transactions

Methodology

The analytical research is directed on learning the provisions of the Digital Personal Data Protection Act published in the Official Gazette of India. The emphasis of the study is to assess the coverage of the act on the various aspects of digital transactions on fintech platforms such as data privacy, data storage, cyber security and network robustness.

Literature Review

Digital Disruptions

‘Disruptive innovations’ have been referred to the transformation in the operation of the business due to the intrusion of technology. The traditional financial system is plagued with emerging digital

innovations of artificial intelligence, blockchain technology, cloud computing which has changed the financial services scenario. (Elia, G., Stefanelli, V. and Ferilli, G.B. (2023)).

The radical changes in the financial services due to the intervention of technology may be understood as digital disruption. Electronic Fund Transfer, cashless payments, credit, debit and prepaid cards, e-wallets, bill payments, ticket bookings are different forms of digital payments. The credit scores of an individual of their banking trajectory are based on the sharing of the digital data. According to a report from Mckinsey's there are seven aspects of digital technology that will shape the landscape of fintechs. They are artificial intelligence, cloud computing, blockchain technology, internet of things, open-source software, serverless architecture and software as a service, no and low code development platforms and hyper automation. Some of the instances of digital disruptions are realized in the following instances:

Open Financial Data: Financial data of an individual is confidential. The spending, savings, investment and borrowings are recorded and maintained by the banks. Such financial data is now open to third parties leading to open financial data.

Financial API: Financial Application Programme Interface connects with other applications safely and shares all the financial data with other applications.

Mobile applications and Web-based Solutions: These provide the customers with hassle free financial transactions in the form of payments or investment, thus tracking the financial habits of the individuals.

Embedded financing: This refers to the financial services offered to the customers through a non-financial product and services. Powered by the API, they are able to track and use the data of the customers to other e-commerce platforms.

Novel business models: Certain business offer loyalty RFID cards which can be used by the customers across the chain of stores. This card captures the spending habits and provides insights on target marketing and niche marketing.

Fintech

'Financial Technology' or 'Fintech' refers to the delivery of financial solutions through technological assistance. Fintech today comprises five major areas: (1) finance and investment, (2) operations and risk management, (3) payments and infrastructure, (4) data security and monetization, and (5) customer interface.

Finance and Investment: The predominant step of technology was in the finance sector. Currently, the major avenues of investment namely, shares, mutual funds, insurance and wealth management services leveraged on the advancing technology and reaped the magnanimous benefits. The emerging area of cryptocurrencies backed by blockchain technology and the counter development of digital currencies by the Central Banks across the world indicates the pros and cons of technological advancements.

Operations and Risk Management: The IT revolution contributed to digital disruption as the financial service companies invested a significant amount in ERP softwares to mitigate risk and enhance operational efficiencies. As a consequence, it led to unperturbed delivery of products and services and a paradigm shift in functioning of businesses.

Payments and infrastructure: Payments across the border aided by the advancements in internet and technology contributed in the digital disruptions. Foreign exchange and electronic fund transfers caused the enormous growth in the fintechs.

Data Security and monetization: Digitisation of transactions and supporting infrastructure has made the fintechs susceptible to cyber-attacks. The rising digital transactions and the voluminous data generated escalate the need for robust and vigilant monitoring systems.

Customer interface: Providing smooth and user-friendly experience will be the core focus of the commercial and IT companies. The competitive edge will lead to the integration of the financial and technology companies, subsequently leading to the development of novel technologies and products.

The Act

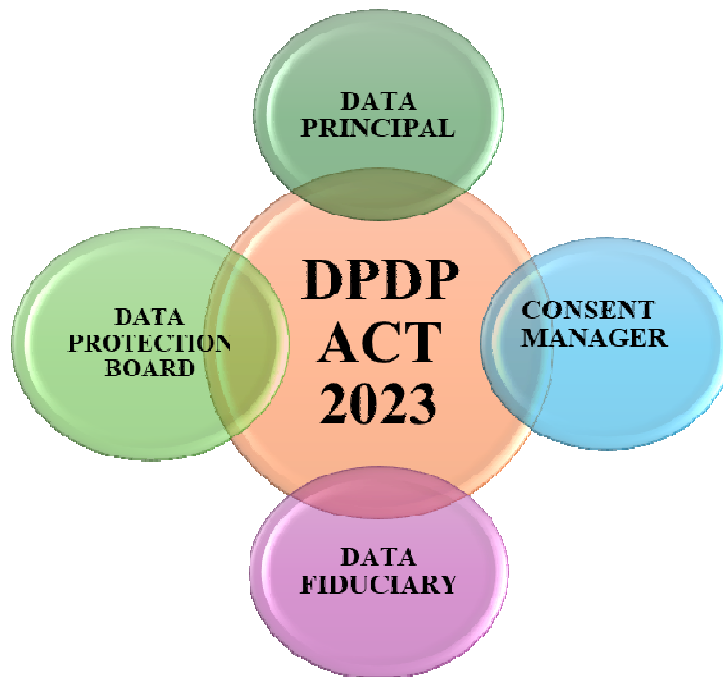
The Digital Personal Data Protection Act 2023 has been scrutinized and the following key observations were made. Sengar, S. S. (2024) emphasizes the enactment is a pivotal milestone which safeguards the netizens interest and the enormous data generated by the transactions. It's a breakthrough achieved by the government to overcome the loopholes of the previous bills and a crucial step towards data privacy.

Naithani, P. (2024). Provides an analysis of Indian Digital Personal Data Protection Act, 2023 in the light of the American Privacy Rights Act of 2024 (2024) and the EU General Data Protection Regulation (GDPR). In the evaluation of the DPDP Act, 2023 it must be noted that there is a need to protect sensitive personal data and the obligation on the part of data fiduciary in processing such data. Ethical obligation with regard to supervision, collection and processing of data has to be imposed on the data fiduciary. The act must safeguard the data principal harm or damages caused by the publicly available information and consent must be obtained for the necessary data and not to collect and process irrelevant data. The act must ensure that continuity of the services to the data principal without any interruption in the prospect of withdrawal of consent to share the data.

Provisions of the Digital Personal Data Protection Act, 2023

The Act has been implemented with the primary objective of protecting the confidentiality of the personal data of a consumer. The preamble of the Act is 'to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.'

The augmentation of technology from being a transmitter of services to predominant necessity led to the enactment. The infinite use of digital technology encompassing the e-commerce, financial service sectors like banks, insurance, mutual funds, stock markets and non-banking companies, government civil services, payment on UPI's, utility bills, healthcare services have all collected the personal data of an individual. The data might be collected with consent or without the active knowledge of the individual.



Important Definitions: Section 2 of the Act provides the following definitions:

Sec 2(h) - ‘Data’ means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;

Sec 2(i) - ‘Data Fiduciary’ means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;

Sec 2(j) - ‘Data Principal’ means the individual to whom the personal data relates and where such individual is

A child, includes the parents or lawful guardian of such a child;

A person with disability includes her lawful guardian, acting on her behalf.

Sec 2 (k) - ‘Data Processor’ means any person who processes the personal data on behalf of a data fiduciary.

Sec 2 (g) – ‘Consent Manager’ means a person registered with the Board, who acts as a single point of contact to enable a data principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

Sec 2(n) – ‘Digital Personal Data’ means personal data in digital form

Digital Data and Consent

Section 4 and 5 of the act provides for the grounds for processing the personal data. It specifies the obligation and the responsibility of the data fiduciary to notify the data principal about the processing of personal data.

Section 6 specifies that the personal data from the data principal has to be collected with free, unconditional and unambiguous consent for the certain legitimate purpose. As illustrated in the Act,

in the processing of personal data, if the mobile application takes consent to access the contact list, where the contact list is not necessary for delivering the service, the consent of the data principal shall be limited to necessary information. Similarly, if a website or application in the processing of personal data, takes consent for waiving the right to seek protection under the act, such consent shall be invalid.

This section also provides for withdrawal of the consent by the data principal and binds the data fiduciary to cease processing the personal data within reasonable time. However, the duration to which the data can be retained and processed varies with the business sector. For instance, where a government agency providing the citizens with unique identification numbers or banks where the personal data of the individual is to be retained for the specified number of years beyond the closing of accounts, the data fiduciary shall do so.

Section 8 and 10 provides for the additional obligations of Data Fiduciary, in which a data principal can rectify an incorrect or insufficient data and complete the incomplete personal data records. The act also protects the right of the individual by providing for the right to erase the consented personal data provided earlier, at the desire of the individual, subject to the provisions of data retention.

The key point to be noted is that the Act protects the personal data provided to a business entity or government agency and does not cover the personal data revealed by an individual on the social media platform.

The key aspects with regard to data collection and processing are noted below:

The act is applicable where the personal data of an individual is processed within the territories of India or being transferred across the border by any person based in India to any person outside India.

The personal data collected may be in digital form or in non-digital form and digitized subsequently.

The personal data must be collected after receiving consent from the individual for specified purpose.

Thus, the act encompasses both financial and non-financial sectors which processes the personal data in digitized form for specified business or non-trade purposes.

Rights and Duties of the Data Principal: Section 11-14 empowers the data principal with

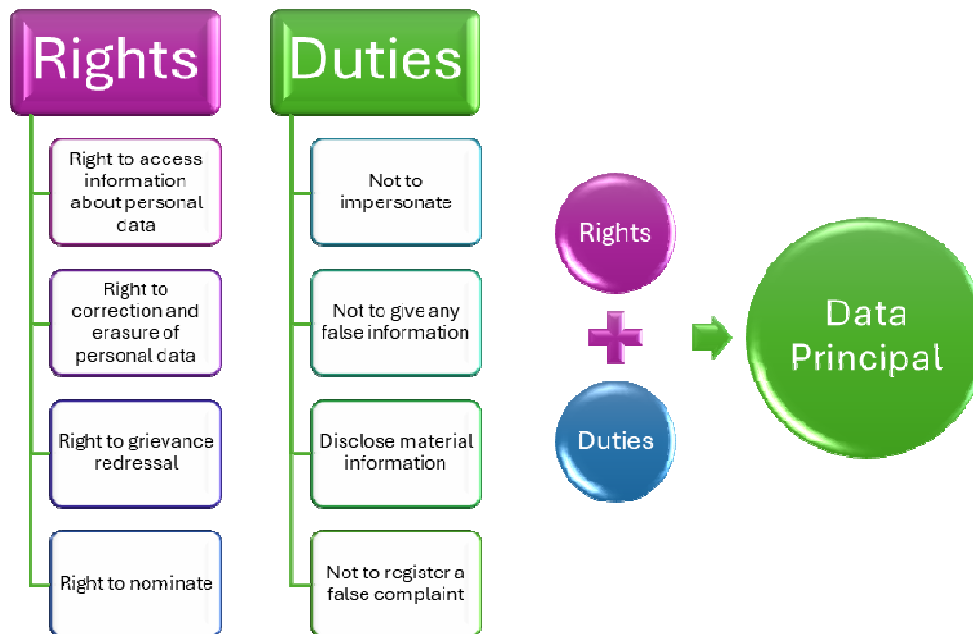
The right to access information about personal data

The right to correction and erasure of personal data

The right of grievance redressal and

The right to nominate

Section 15 spells out the duties of Data principal and mentions that the individual providing data must not impersonate or give false information. They should disclose material information which may bear consequences on the future course of business. It binds the data principal not to register a false complaint.



Establishment of Data Protection Board of India: Section 18 – 26 of the act provides for the establishment of the Data Protection Board consisting of a Chairperson and Members, headquartering as indicated by the Central Government of India.

Section 27 empowers the Board to adjudicate the data breach grievances brought forward by the aggrieved party and mediate between the two parties.

On the receipt data infringement complaint, the board through the Consent manager shall verify the authenticity and the degree of breach.

The board shall give an opportunity to aggrieved party to be heard and determine the grounds to proceed further with an inquiry

The board can summon, enforce the attendance of any person and examine the case.

It can inspect any relevant documents and evidences, but shall not to take into custody any digital equipment that may affect the routine functioning of the person

The Board is authorised to impose penalties if the data breach infringement is proved. Breach of the provisions of the act attracts penalties ranging from Rupees Ten Thousand to Rupees Two Hundred and Fifty Crores.

However, the board is rendered powerless as they are not allowed to seize the digital equipment for any examination. The digital equipment shall remain in the custody of the data processing party so that it doesn't interrupt with the day-to-day functioning of business. Such a clause may increase the difficulties of the authorities of the board in the trial process and may hamper the fair and just procedure required to be followed, as there is ample scope for manipulation of data.

If the aggrieved party is unsatisfied with the verdict of the board, they can approach an Appellate tribunal sixty days post the verdict.

This reduces the status of the board to merely a vigilance authority or an ombudsman.

Discussion

The provision of the act safeguards the digital data of an individual voluntarily provided on any of the fintech platforms. The digital data can be used only for the specified purpose and can be stored for the specified duration or as per the requirements of law in the various businesses. However, the law does not provide for the protection of digital data published by an individual on the digital platforms other than business purposes.

The act focuses primarily on protection of the rights of the data principal in the context of digital data but from the fintech viewpoint, the issues of susceptibility of the digital data to scammers, transfer of digital data between the business houses, cyber-attacks and network vulnerability are not addressed. Certain issues of data collection over website or applications with the aid of API, storing and sharing of such data without the knowledge and consent of data principal has not been given due consideration.

In the context of the fintechs, the law provides safety measures to only a limited part of the transaction. As mentioned above, the large part of the fintech transaction remains unguarded.

Findings

The analysis of the provisions of the act in the light of the fintech and digital disruptions have yielded the following points:

There is a need to broaden the definition of the 'Digital Data Protection' and provide safety to the data principal

There is lack of clarity on the safety of the digital data collected by latent modes without the consent.

The act can be applied to any sector or business house which operates with support technology, irrespective of government or non-government agencies.

The act does not specify the role and responsibility of the Consent Manager.

The Act only provides for the Data Protection Board, but does not mention the number of members to the board and limits their function to monitoring agent.

The act overlooks on the digital data collected through the continuous assessment of technology usage like algorithm, artificial intelligence and machine learning.

Conclusion

India is the largest economy in the digital landscape and accounts for one among the top 5 countries of the world for voluminous digital transactions. A recent data shows that Indians have downloaded 26 billion applications and consume 6.45 hours of internet. The facts and figures evidently demonstrate that changes in digital arena are swiftly accepted by the consumers and fintech landscape has been growing exponentially.

The enactment of the Digital Personal Data Protection Act, 2023 is a remarkable milestone in the era of digital disruptions caused by rapidly advancing technologies. In the light of the enormous digital transactions registering and technological advancements, there is a need for quick response action on the part of the government. The country witnessed technological boom in the early 2000's and the act has been enforced post two decades of the revolution. The data principal has to bank on the cyber and IT laws to address any issue that is beyond the purview of the act.

The government has to take charge of the situation and establish laws covering the areas of digital frauds, transfer of digital data, cyber attacks and robust networks.

References

Elia, G., Stefanelli, V., & Ferilli, G. B. (2023). Investigating the role of Fintech in the banking industry: What do we know? *European Journal of Innovation Management*, 26(5), 1365–1393. <https://doi.org/10.1108/EJIM-12-2021-0608>

Fintech lending – face. (n.d.). Retrieved August 30, 2024, from <https://faceofindia.org/fintech-lending/>

Ministry of electronics and information technology, government of india | home page. (n.d.). Retrieved August 30, 2024, from <https://www.meity.gov.in/>

Naithani, P. (2024). Analysis of india's digital personal data protection act, 2023. *International Journal of Law and Management*. <https://doi.org/10.1108/IJLMA-05-2024-0174>

Reserve bank of india—Reports. (n.d.). Retrieved August 30, 2024, from <https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=892>

Resources – face. (n.d.). Retrieved August 30, 2024, from <https://faceofindia.org/resource-center/>

Sengar, S. S. (2024). From pixels to policies: Analysing the provisions and navigating the complexities of the digital personal data protection act, 2023. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4547842>

Unlock innovation with gff: The fintech blog for industry leaders. (n.d.). Retrieved August 30, 2024, from <https://globalfintechfest.com/blog>

What is fintech? 6 main types of fintech and how they work. (n.d.). Plaid. Retrieved August 16, 2024, from <https://plaid.com/resources/fintech/what-is-fintech/>

What is fintech (Financial technology)? | McKinsey. (n.d.). Retrieved August 16, 2024, from <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-fintech#/>

Websites:

<https://dea.gov.in/sites/default/files/Report%20of%20Indias%20G20%20Task%20Force%20On%20Digital%20Public%20Infrastructure.pdf>

https://faceofindia.org/wp-content/uploads/2024/08/Edited-Cube_Issue-4_Aug-2023_final_1st-August-1.pdf

<https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>