 DOI: 10.5281/zenodo.17393246

DATA PRIVACY: IMPACT OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023 ON INDIAN STARTUP

BY SOUMYA PRAKASH HOTA[1] & PRATYUSHA PUROHIT[2]

Abstract

The goal of the Digital Personal Data Protection (DPDP) Act, 2023, is to ensure that businesses handle data in a way that protects people's security and privacy by establishing a progressive legal framework that regulates the collection, storage, and transfer of digital personal data. By imposing severe penalties and measures, the Act tackles the problem of data breaches among Indian startups. Specifically, companies could be fined up to INR 200 crores for failing to notify authorities of a data breach and up to INR 250 crores for failing to implement reasonable security measures. The law requires data fiduciaries (businesses) to take safety measures, report incidents to the Data Protection Board, and follow guidelines such as data minimization, which calls for collecting only the most important data and deleting it after use. Stakeholders, however, are worried that the new regulations may significantly limit cross-border data transfers, which could result in increased compliance expenses and regulatory barriers that could impede startups' ability to expand and compete.

[1] The author (I) is a law student at Birla Global University.
[2] The author (II) is a law student at Birla Global University.

 DOI: 10.5281/zenodo.17393246

INTRODUCTION

This act was introduced primarily to control how digital personal data is handled and make sure it is utilized responsibly. The purpose of the act is to provide a progressive legal structure that controls how personal data is gathered, stored, and transferred. By doing this, it aims to ensure that businesses handle data in a way that protects people's security and privacy. This all-encompassing strategy aims to safeguard personal data against misuse and guarantee that it is managed in an authentic and accountable manner.

The research make use of mixed -method approach , combining the Quantitative and Quantitative methods to comprehensively analyze the Digital personal Data protection ,2023 effectively will address the issue of data breach among Indian Startup .The study focus on understanding the trend of trends in data breach incidents among Indian startups, the anticipated challenges due to the Personal Data Protection (PDP) Bill, and whether the Bill effectively addresses these issues.

Douwe Korff; The Indian Digital Personal Data Protection Act, 2023, viewed from a European perspective; SSRN ;2023[3]

The study paper by Douwe Korff looks at the Digital Personal Data Protection Act,

2023 in India from a European standpoint. International law expert Korff assesses how well the DPDP Act complies with European data protection regulations and considers how it would affect data privacy and cross-border data transfers between India and the EU. In addition, Korff talks about how the DPDP Act affects national security, research data, and European Commission data adequacy rulings. In summary, the study offers an in-depth examination of the legal and regulatory framework pertaining to data protection in Europe and India, emphasizing the challenges associated with standardizing data protection guidelines among diverse legal systems.

[3] Douwe korff, 'The Indian Digital Personal Data Protection Act, 2023, viewed from a European perspective' SSRN(2023) SSRN 4614984

Personal Data protection Bill on the Startup Ecosystem ;The Dialogue ;2021[4]

This study intends to highlight the provisions of the 2019 Personal Data Protection Bill and the ways in which the startup ecosystem will be affected by the bill once it becomes law. Using empirical methodologies, this study involved interviews with five consulting firms and fifty-seven startups. These are the main conclusions: Clear processes and limitations should be established for government agencies to safeguard the business interests and privacy rights of startups. The operations of startups can be improved by encouraging active collaboration among various regulatory entities. The definition of data should be precise and clear, with a narrower definition of sensitive data categories. The Data Protection Authority (DPA) and other entities like TRAI and CCI should be coherent and consistent in their data protection regulatory bodies. and small businesses; furthermore, cooperation and alignment between regulatory organizations will establish a regulatory environment that fosters the growth and endurance of startups in the age of digital commerce. The goal of these suggestions is to improve the startup-friendly regulatory landscape by safeguarding privacy and encouraging development and innovation.

History of DPDP Act 2023

The Supreme Court rendered a significant ruling in the matter of Justice K.S. Puttaswamy v. Union of India[5] in 2017. The nine justices of the Supreme Court assembled to decide whether or not the right to privacy is guaranteed by the constitution. The nine-judge panel unanimously upheld the Constitution's fundamental right to privacy, right to privacy as fundamental rights under the constitution within Article 21 in particular and Part III in whole. The rulings in the cases of Kharak Singh and M.P[6]. Sharma was overturned.

An expert group was formed by the Union Ministry of Electronics and Information Technology to investigate and pinpoint the most important data protection issues following the August 2017 ruling. This committee[7] comprised representatives from the government, academia, and business, and it was chaired by retired Supreme Court Justice B.N. Srikrishna. While preparing a report to address issues with India's data system, the committee overlooked key crucial details

[4] The dialogue, IMPACT STUDY:PERSONAL DATA PROTECTION BILL ON THE START-UP ECOSYSTEM,2019

[5] Justice KS Puttaswamy v Union of India AIR 2017 SCC 1

[6] Kharak Singh v state of UP 1964 1SCR 332

[7] Ministry of Eletronics and Information “A Free and Fair Digital Economy” committee

that are necessary for robust data protection. In contrast to the principle of informed consent established in the 2017 Puttaswamy ruling, it permitted the government to utilize personal data without consent in order to offer services.

Additionally, the bill does not address the necessity of changing the rules governing surveillance, which means that there is little supervision of government spying. Greater privacy issues might arise if all data were stored in India without altering surveillance regulations. The Personal Data Protection Bill 2019 was then presented in

Parliament but was eventually withdrawn. After two years, the Joint Parliamentary Committee[8] that was tasked with overseeing it made recommendations for modifications to the 2019 bill. After reviewing the suggestions, the Ministry of Electronics and Information Technology reviewed the recommendations, and in 2022, the committee released the Digital Data Protection Bill in November. The bill was finally passed by Parliament in July 2023.

Historical Trends in Data Breach Incidents

Everybody in the modern day is digitizing their enterprises, and in this globally networked environment, cyberattacks on startups and businesses have grown significantly. India is not behind. A startup that has a data breach may face a number of challenges, including compromised client privacy and large financial damages. Because they don't have well-established security protocols, startups are more susceptible to data breaches. Numerous high-profile data breaches affecting Indian businesses, including Bigbasket, Unacademy, Juspay, and Dunzo, have occurred in recent years[9]. One of the top ed-tech platforms in India, Unacademy[10], for instance, experienced a security breach in [11] that resulted in the exposure of about 20 million subscribers' data. The attackers asserted to possess the company's complete database. Another story involves a data leak that affected 3.4 million users of the grocery

[8] Indranath Gupta "An Assessment of the JPC Report on PDP Bill, 2019" 2022 Economic and Political Weekly (Engage), Vol. 57

[9] Ashish Tandon, "Impact of cyber attacks on startups and how founders can protect their businesses"(Economic Times ,Aug 22 ,2022)<https://cio.economictimes.indiatimes.com/amp/news/digital-security/impact-of-cyber-attacks-on-startups-and-how-founders-can-protect-their-businesses/93700124> Accessed 22 Aug 2022

[10] Abhijit Ahakar "Millions of Unacademy user accounts exposed in data breach:(Mint 6 May

[11])<https://www.livemint.com/technology/tech-news/over-20-mn-unacademy-user-accounts-exposed-in -data-breach-report/amp-11588775083410.html> 6 may 2020

delivery firm Dunzo[12][13]. Information about the last login, phone model, and location was made public. These represent only a small selection of cyberattacks and data breaches.
Comprehensive legislation pertaining to data protection were not in effect at that time.

All of that has changed, though, with the passage of the Digital Personal Data Protection Law in 2023 and its scheduled implementation in July of 2024. For both individuals and corporations, data breaches are a major worry. Companies may incur additional expenditures for data security, litigation, and other fees as a result of security breaches. Breach can harm GDP, threaten national security, and expose personal information to compromise. A company's reputation can also be harmed by data leaks, and destroy customer trust, which is particularly harmful to startups.

Overview of the Personal Data Protection (PDP) Bill

The purpose of the DPDP Act was data protection. This act's justification includes outlining the responsibilities and rights of data fiduciaries[14] and data principals, as well as penalizing data breaches. The primary goals of the legislation are to ensure that consent is available in all languages, erase data once its intended use has been completed, and restrict data acquisition to what is absolutely essential.
Data fiduciaries, or businesses, startups, and corporations that gather data from data principals (i.e., consumers), are covered under a number of different regulations. Data fiduciaries are required to put safety precautions in place to stop data breaches and notify the Data Protection Board of any such incidents.
All businesses, including startups, must also assess their data procedures to guarantee adherence to the Digital Personal Data Protection.

Potential impact of DPDP on startup

Organizations are required by the DPDP Act to take all appropriate steps to safeguard data against hacking and breaches. The act intends to raise accountability for companies in charge of any breaches and drastically lower the danger of breaches involving personal data. It pushes

[12] Prasid Banerjee “Dunzo data breach contained personal information of over 3 million accounts”29 Jul
[13] <https://www.livemint.com/technology/tech-news/dunzo-data-breach-contained-personal-information -of-over-3-million-accounts/amp-11596019951200.html> 29 Jul 2020
[14] The Digital Personal Data Protection Act ,2023 S2

businesses to give data protection first priority and establishes penalties for breaking the security procedures specified in the act. Startups and businesses risk fines of up to INR 250[15] crores for failing to put reasonable security measures in place, and they risk fines of up to INR 200[16] crores for failing to notify the authorities of any data breach. Reducing data breaches and restoring customer trust in digital services are the goals of these severe fines and regulations. Startups can take the following actions to prevent data breaches: Strong policies that outline the procedures for gathering, storing, and using data are essential. Data minimization is applied, with only the information needed and deleted after use. Regular assessments are carried out to identify present or potential threats, and data is safeguarded with strong security measures. Appropriate resources and employee training are also provided to prevent phishing and other forms of attacks, and a solid backup plan is created to determine where to store data in the event of a breach. Startups can strengthen their defenses against data breaches by implementing these strategies.

Stakeholder Perspective

The Dialogue recently hosted a conference to address concerns about the impact of new data transfer restrictions on 57 startups. They think that new rules may severely restrict the movement of data across borders, which would make it more difficult for startups to utilize international data centers and cloud services. As a result, these businesses may incur higher expenses in their efforts to meet the strict data transmission regulations.In addition, the new rules provide the government the power to access any company's non-personal and personal data for planning and policy-making reasons. This degree of access may violate third parties' intellectual property rights and other legal protections if appropriate precautions aren't in place. There are grave worries over the possible detrimental effects on innovation and impact on innovation and invention within the startup ecosystem.

One major concern is that increased compliance costs and regulatory hurdles could hold back the growth and competitiveness of startups. Many startups rely on the ability to freely access and transfer data across borders to leverage advanced cloud computing resources and collaborate with international partners. Restrictions on data flow could hinder these

[15] The Digital Personal Data Protection Act,2023 Schedule 1

[16] The Digital Personal Data Protection Act,2023 Schedule 2

 DOI: 10.5281/zenodo.17393246

capabilities, making it more challenging for startups to scale their operations and compete in the global market.

Critical Analysis

In my view, the Digital Personal Data Protection Law will have a significant impact on data breaches and cybersecurity. I believe that this legislation will reduce the frequency of data breaches by compelling companies to adopt more strong data security measures and handle data with greater care. The law's emphasis on stringent penalties for non-compliance is likely to motivate organizations to prioritize data protection.

Data minimization, which requires businesses to gather just the minimal amount of data required for their operations and guarantee that it is erased after use, is one of the fundamental ideas emphasized by this regulation. This concept not only protects individual privacy but also decreases the possibility of data being breached. Businesses may reduce the quantity of data they keep by restricting the Potential harm from any data breaches that could take place.

the legislation promotes the adoption of thorough data protection measures by businesses, such as staff training programs, frequent security assessments, and encryption. These actions are critical to establishing a data security culture in businesses by making sure that all staff members are aware of the critical nature of safeguarding personal information and the dire repercussions of not doing so.

Bibliography

(1) Douwe korff, 'The Indian Digital Personal Data Protection Act, 2023, viewed from a European perspective' SSRN(2023) SSRN 4614984

(2) The dialogue, IMPACT STUDY:PERSONAL DATA PROTECTION BILL ON THE START-UP ECOSYSTEM,2019

(3) Justice KS Puttaswamy v Union of India AIR 2017 SCC 1

(4) Kharak Singh v state of UP 1964 1SCR 332

(5) Ministry of Eletronics and Information "A Free and Fair Digital Economy" committee

(6) Indranath Gupta "An Assessment of the JPC Report on PDP Bill, 2019" 2022 Economic and Political Weekly (Engage), Vol. 57

(7) Ashish Tandon, "Impact of cyber attacks on startups and how founders can protect their businesses"(Economic Times ,Aug 22 ,2022)<https://cio.economictimes.indiatimes.com/amp/news/digital-security/impact-of-cyber-attacks-o n-startups-and-how-founders-can-protect-their-businesses/93700124> Accessed 22 Aug 2022

(8) Abhijit Ahakar "Millions of Unacademy user accounts exposed in data breach:(Mint 6 May 2020)<https://www.livemint.com/technology/tech-news/over-20-mn-unacademy-user-accounts-e xposed-in-data-breach-report/amp-11588775083410.html> 6 may 2020

(9) Prasid Banerjee "Dunzo data breach contained personal information of over 3 million accounts"29 Jul 2020<https://www.livemint.com/technology/tech-news/dunzo-data-breach-contained-personal-in formation-of-over-3-million-accounts/amp-11596019951200.html> 29 Jul 2020

(10) The Digital Personal Data Protection Act ,2023 S2

(11) The Digital Personal Data Protection Act ,2023 Schedule 1

(12) The Digital Personal Data Protection Act ,2023 Schedule 2

(13) Akshayy Nanda , 'From Crisis to Control: How the Digital Personal Data Protection Law Curbs Data Breaches' (Medianama May 22

2024)<https://www.medianama.com/2024/05/223-dpdp-act-databreaches#:~:text=This%20includes%20notifying%20affected%20individuals,provided%20in%20the%20awaited%20rules.> may 22 2024

(14) Anirudh Burman , 'Understanding India New Data Protection Law '

(Carneige ,Oct

3,2023)<https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protect ion-law?lang=en>oct 3 ,2023

(15) Mohan , '**Exemptions Denied: The Impact of the New Privacy Law on Startups'(Data track ,Jan 15**

2024)<https://www.datatracks.com/in/blog/the-impact-of-the-new-privacy-law-on-startups/ >

June 12,2024

(16) Arohana , 'Background of Data Protection Laws in India'(Arohana legal ,May 6,2024)<

https://arohanalegal.com/startups/data-protection-laws-for-startups/ >