RESEARCH ARTICLE OPEN ACCESS

Data Privacy and Security Policies in India

Moin Malek[1], Jaimin Kapadiya[2], Debraj Maji[3] and Kusum Lata Dhiman[4]
1(Dept. Cyber security and Forensics, Parul University, India
Email: 210305126701@paruluniversity.ac.in)
2(Dept. Cyber security and Forensics, Parul University, India
Email: 210305126707@paruluniversity.ac.in)
3(Dept. Cyber security and Forensics, Parul University, India
Email: 200305126023@paruluniversity.ac.in)
4(Dept. Computer Science & Engineering, Parul University, India
Email: kusumlata.dhiman21133@paruluniversity.ac.in)

Abstract:

In today's world of smartphones and social media, our personal information continuously goes through the digital world. This data, from our browsing habits to our online purchases, makes a very carefully detailed picture of who we are. Just like we wouldn't leave our personal belongings like wallets or passports lying around, this digital information needs protection. Data privacy empowers us to control our digital footprint. It's about knowing what information is collected about us, who has access to it, and how it's being used. Imagine data privacy as a lock on your digital locker – it allows you to decide who gets the key and what they can see inside. This control ensures transparency and empowers you to make informed choices about how your information is used. Data security, on the other hand, focuses on safeguarding this digital information itself. It's like building a strong wall around your locker. Robust security measures like encryption and access controls act as guards, preventing unauthorized access or misuse of your data. Strong data security protects you from dangers like identity theft and financial fraud, where criminals might steal your information for malicious purposes.

Now, let's explore the role of the law in protecting our digital selves. India, like many countries, has recognized the importance of data privacy and security. The government has established policies and regulations to safeguard citizens' information. These policies outline the rights individuals have over their data and the responsibilities organizations must uphold when handling personal information. Understanding these policies empowers you to hold organizations accountable and make informed decisions about the information you share online.

I. INTRODUCTION

In today's digital world, data privacy and security are two sides of the same coin, crucial for protecting your personal information. Imagine your data as a collection of personal belongings. Data privacy focuses on your control over these belongings, ensuring transparency about who has access, how they're used, and for what purpose. You have the right to know what information is collected about you, control how it's used, and even request its deletion in certain situations.

Data security, on the other hand, is like building a safe around your belongings. It focuses on protecting your information from unauthorized access or misuse. This involves strong measures like passwords, access controls, and encryption to ensure confidentiality, integrity, and availability of your data.

Figure 1: Data Privacy and Security

Examples include social media platforms allowing you to adjust privacy settings (data privacy) and banks using encryption to protect your financial information (data security).

Both aspects are vital for several reasons. Securely stored data protects you from identity theft and fraud, safeguards sensitive information like medical records, empowers you with control over your information, and builds trust in the digital world. Balancing these needs with innovation is a challenge. Businesses need data to operate, but also have a responsibility to protect it. Governments play a crucial role in establishing regulations that ensure both individual rights and economic growth.

Ultimately, understanding data privacy and security empowers you to make informed decisions about how you share your data and advocate for strong data protection practices, safeguarding your information in the digital age.

II. WHY IS IT NECESSARY?

Figure 2. Requirement of data privacy and security

Data privacy and security have become important for safeguarding our online lives. Imagine your personal information as a collection of treasured belongings. Data privacy grants you control over these "belongings," making certain transparency in who has access, how they're used, and for what purpose. This authorizes you to understand what information is collected about you, control how it's utilized, and even request its deletion in certain situations.

Data security, on the other hand, acts as a fortress protecting these "belongings." It focuses on safeguarding your information from unauthorized access or misuse. This includes robust measures like strong passwords, access controls, and encryption to guarantee the confidentiality, integrity, and availability of your data.

While conceptually distinct, data privacy and security are inextricably linked. Without robust security measures in place, ensuring true control over personal information becomes virtually impossible. Strong data security practices function as the essential foundation upon which data privacy rights can be effectively upheld.

The necessity of both data privacy and security stems from the very real dangers lurking in the digital landscape. Data breaches, unauthorized access, and misuse of information can have devastating consequences, ranging from financial ruin and identity theft to privacy violations and a loss of control over your digital self.

Furthermore, data security safeguards not only personal details but also highly sensitive information like medical records, financial data, and private communications. This protection is crucial for maintaining healthcare privacy, preventing financial losses and fraud, and building trust in institutions that handle such sensitive information.

Beyond protection, data privacy empowers you to take control of your digital footprint. You gain the right to know who collects your data, why they need it, and how it will be used. This knowledge allows you to make informed decisions about sharing your information and setting appropriate privacy preferences, ultimately shaping your online experience.

However, achieving the ideal balance between data-driven innovation and individual security requires a collective effort. Individuals need to be mindful about the information they share online and advocate for strong data protection measures. Organizations must implement robust security

practices, respect user privacy, and be transparent about data collection and usage. Finally, governments play a critical role in establishing regulations that promote innovation while protecting individual rights and ensuring responsible data practices.

III. Current Policy and how it differs from earlier ones.

The Data Protection and Privacy Act of 2023 (DPDP Act) marks a significant turning point in India's legislative landscape, indicating a new era of comprehensive data protection and privacy governance. With the exponential growth of digital transactions and online interactions, the need to protect individuals' privacy rights and minimize risks associated with data misuse has become increasingly noticeable. In response to these necessities, the DPDP Act represents a concerted effort to modernize India's data protection control, aligning it with international best practices while addressing the unique cultural, economic, and technological realities of the country.

Compared to previous Acts, such as the Information Technology (IT) Act of 2000 and the proposed Personal Data Protection Bill (PDPB), the DPDP Act symbolizes a apparent shift in India's approach to data governance. While the IT Act laid down fundamental provisions for data protection and cybersecurity, its scope and enforcement mechanisms were deemed inadequate to address the evolving challenges posed by digital technologies and global data flows.

The proposed Personal Data Protection Bill (PDPB), which underwent several iterations and consultations, represented a step forward in expressing comprehensive principles and rights for data subjects and obligations for data fiduciaries. However, its enactment faced delays and criticisms regarding certain provisions, including concerns over data localization requirements, exemptions for government data processing, and ambiguity regarding consent mechanisms.

In contrast, the DPDP Act seeks to address these gaps by introducing an in depth framework encompassing principles of transparency, accountability, data minimization, purpose limitation, and user consent. One of the salient features of the DPDP Act is its emphasis on empowering individuals with greater control over their personal data, promoting trust and accountability in the digital ecosystem. By mandating clear and explicit consent mechanisms, data subjects are empowered to make informed choices regarding the collection, processing, and sharing of their personal information.

Moreover, the DPDP Act incorporates provisions for robust enforcement and regulatory oversight, including the establishment of a Data Protection Authority (DPA) tasked with monitoring compliance, adjudicating disputes, and imposing penalties for non-compliance. This represents a significant departure from previous laws, which often lacked adequate enforcement mechanisms, resulting in a culture of impunity for data breaches and privacy violations.

The Data Protection and Privacy Act of 2023 (DPDP Act) differs from previous laws, such as the Information Technology (IT) Act of 2000 and the proposed Personal Data Protection Bill (PDPB), in several key aspects, such as:

1. Comprehensive Framework:

Compared to the IT Act, which primarily focused on aspects of electronic commerce and cybersecurity, the DPDP Act provides a comprehensive framework specifically dedicated to data protection and privacy. It addresses a wide range of issues related to the collection, processing, storage, and sharing of personal data, ensuring a more in depth approach to data governance.

2. Focus on Individual Rights:

While the IT Act laid down basic provisions for data protection, the DPDP Act places a stronger emphasis on individual rights and empowerment. It grants individuals more control over their personal data by allowing them to make informed decisions about how their data is used and shared.

3. Clear Authorization Mechanisms:

Unlike previous laws, which may have had vague or ambiguous authorization requirements, the DPDP Act mandates clear and explicit consent mechanisms. This ensures that individuals are fully aware of the purposes for which their data is being processed and have the opportunity to opt out if they so choose.

4. Robust Enforcement Mechanisms:

One of the notable differences with the DPDP Act is the introduction of robust enforcement mechanisms, including the establishment of a Data Protection Authority (DPA). The DPA is tasked with monitoring compliance, adjudicating disputes, and imposing penalties for non-compliance, providing a data protection framework.

5. Risk-Based Approach:

The DPDP Act adopts a risk-based approach to data protection, recognizing that not all data processing activities pose the same level of risk to individuals' privacy. By categorizing data into different risk tiers and prescribing corresponding safeguards and obligations for data fiduciaries, the DPDP Act ensures a more tailored approach to privacy protection.

However despite these benefits it does have several drawbacks, such as:

1. Does not cover offline personal data and non-automated processing.
2. Comparing it to the General Data Protection Regulation (GDPR), Penalties under the DPDP Act extend up to INR250 crore, Penalties under GDPR extend to 20 million euros, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.
3. The Act does not specify a timeframe for Personal Data breach notification.
4. The Act comprises an additional right to nominate while omitting the right to portability and timeline to respond to the Data Principal requests has not been specified.
5. The Act does not include any obligation for Data Fiduciaries to maintain records of processing activities (ROPA).
6. The Act has not identified any transfer mechanisms for transferring Personal Data.
7. Does not provide 'Right to data portability' and 'Right to be forgotten' while both previous DPDP 2018 and PDP 2019 did have this Rights.
8. Does not specify harms of processing of personal data unlike previous bills like monetary loss, identity theft, loss of reputation and unreasonable surveillance.

IV. CONCLUSION

In conclusion, the enactment of the Data Protection and Privacy Act of 2023 (DPDP Act) marks a decisive moment in India's journey towards establishing a robust and comprehensive framework for data protection and privacy. This legislation represents a significant departure from previous laws, such as the Information Technology (IT) Act of 2000, by providing a more nuanced, rights-based, and enforceable approach to safeguarding individuals' privacy rights in the digital age.

The DPDP Act stands out for its focus on individual empowerment, as evidenced by the introduction of explicit consent mechanisms and enhanced rights for data subjects. By granting individuals greater control over their personal data and ensuring transparency and accountability in data processing practices, the DPDP Act fosters trust and confidence in India's digital ecosystem.

However, the successful implementation of the DPDP Act will depend on effective collaboration and coordination among government agencies, regulatory bodies, businesses, civil society organizations, and individuals. It will also require ongoing adaptation and evolution to keep pace with technological advancements, emerging threats, and evolving societal norms.

REFERENCES

1. *PRS India, "The Digital Personal Data Protection Bill, 2023".*
2. *Meity.gov.in "Digital Personal Data Protection Act 2023 | Ministry of Electronics & Information Technology, Government of India".*
3. *Wikipedia "The Digital Personal Data Protection Bill, 2023".*
4. *Press Information Bureau "Salient Features of the Digital Personal Data Protection Bill, 2023".*
5. *Bar and Bench "Digital Personal Data Protection Act, 2023 – A Brief Analysis".*
6. *Anirudh Burman – Carnegie India "Understanding India's New Data Protection Law".*
7. *PwC India "The Digital Personal Data Protection Bill, 2023".*
8. *Cyril amarchand mangaldas "The DPDP Bill Overview: A New Dawn for Data Protection in India"*
9. *Grant thornton "Data Protection Act 2023's Impact on Consumer Businesses: The Way Forward".*
10. *Secure privacy "What Data is Protected by the India Digital Personal Data Protection Act 2023? A Comprehensive Guide to the India Data Privacy Law".*
11. *Nishith desai associates "INDIA'S DIGITAL PERSONAL DATA PROTECTION ACT, 2023: HISTORY IN THE MAKING".*
12. *Times of India "Digital Personal Data Protection Act 2023 – A game changer*