AG Publishing House

Transformative Constitutionalism: Issues and Challenges

Volume 1
Year: 2025

AG PH Books

Protection of Data Privacy under Digital Personal Data Protection Act, 2023: A Critical Legal Analysis

Dr. Mujibur Rehman[1], Maria Momin[2]

[1]*Assistant Professor, Department of Law, School of Legal Studies, BBAU, Lucknow*

[1]*Research Scholar, Department of Law, SLS, BBAU, Lucknow*

Abstract

Data privacy is an increasingly significant and complex issue in today's digital age. It is a fundamental aspect of our digital lives, protecting our personal information from misuse and abuse. In India, the Digital Personal Data Protection Act of 2023 marks a significant milestone in the evolving landscape of data privacy and protection. It is designed to tackle the growing concerns surrounding the handling of personal data in the digital age. It sets forth a comprehensive framework that empowers individuals with greater control over their personal information. Central to this Act is the acknowledgment of data privacy as a fundamental right, in alignment with international standards and best practices. While Digital Personal Data Protection Act of 2023 is a substantial leap forward in safeguarding data privacy, nevertheless, challenges persist. Balancing the needs of innovation and business with the imperatives of data protection remains an ongoing concern. Moreover, effectiveness of the Digital Personal Data Protection Act of 2023 signifies a crucial step toward fortifying data privacy rights in the digital era. By codifying fundamental principles and establishing stringent mechanisms for enforcement, it aims to protect individuals' personal data while fostering a conducive environment for innovation and technology-driven growth. Its impact will depend on rigorous implementation and continuous adaptation to the dynamic landscape of digital data. In this chapter, the authors critically analyse the personal data breaches by regulatory authority and aim to build a data protection framework that would regulate processing of personal data by government and non-government entities in light of right to privacy judgment under the Digital Personal Data Protection Act, 2023.

Keywords: Digital Personal Data Protection Act 2023, Data Privacy in India, Right to Privacy, Personal Data Regulation, Data Protection Framework

1 Introduction

In our increasingly interconnected and digitized world, the protection of data privacy has emerged as a paramount concern for individuals, businesses, and governments alike. As technology continues to advance at an unprecedented pace, the need for comprehensive legal frameworks to safeguard personal

data has become ever more pressing. In response to this imperative, the Digital Personal Data Protection Act of 2023 has taken centre stage as a critical legal instrument designed to tackle the intricate challenges posed by data privacy in the digital age.[1]

This legislation marks a significant milestone in the on-going evolution of data protection laws, reflecting an earnest attempt to adapt to the complexities of our modern information ecosystem. The Digital Personal Data Protection Act, 2023, recognizes the fundamental importance of safeguarding individuals' personal information, while striving to strike a delicate balance between innovation and economic growth and preserving fundamental right to privacy.

In this critical legal analysis, we will delve deep into the intricacies of this legislation, examining its key provisions, enforcement mechanism, and potential implications. We will scrutinize the Act's effectiveness in safeguarding data privacy, evaluating its alignment with international standard and principles. Furthermore, we will explore the practical challenges and ethical dilemmas that may arise in its implementation, seeking to unravel the multifaceted layers of this legal framework.

2 Data Privacy: Theoretical and Conceptual Framework

Data privacy is a multifaceted and critical aspect of our contemporary digital world. As the volume of personal data generated, collected, and disseminated continues to grow exponentially, the need for a robust theoretical and conceptual framework to address data privacy concerns becomes increasingly imperative. Some of its aspects which are the part of its conceptual framework are as follows:

2.1 The philosophical foundation of data privacy

At the heart of data privacy lays a philosophical question: What rights do individuals have over their personal information? Philosophers like John Locke and Immanuel Kant have contributed to the development of theories related to individual autonomy and personal property. Locke's concept of self-ownership and Kant's emphasis on human dignity provide the groundwork for understanding data privacy as an extension of personal autonomy. In this context, data privacy can be seen as the right of individuals to control and protect their personal information, akin to their rights over physical property.[2]

2.2 The legal foundations of data privacy

Legal frameworks are instrumental in defining and safeguarding data privacy rights. Various nations and regions have enacted legislation to protect individuals' personal data. The European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are notable examples. These laws establish principles such as data minimization, purpose limitation, and transparency, forming the basis for how organizations should handle personal data. They also grant

[1]Gwen Kennedy, *Data Privacy Law: A Practical Guide to the GDPR* 14 (Amazon Digital Services LLC-KDP, 2019).
[2]Nataraj Venkatraman and Ashwin Shriram, *Data Privacy Principle and Practise* 5 (CRC Press Publications, 2016).

individuals rights like the right to access their data, the right to be forgotten, and the right to data portability.

2.3 Ethical consideration in data privacy

Ethics plays a crucial role in shaping the framework for data privacy. It raises questions about what is morally right or wrong when it comes to handling personal data. The ethical principles of transparency, fairness, accountability, and consent are central to data privacy discussions. For instance, obtaining informed and explicit consent before collecting personal data is seen as an ethical imperative. Ethical considerations also extend to data breaches, algorithmic bias, and the responsible use of data in emerging technologies like artificial intelligence.

2.4 The role of technology in data privacy

Technology both challenges and enables data privacy. On one hand, technological advancements have made it easier to collect, store, and analyze vast amounts of personal data, often without individuals' knowledge or consent. On the other hand, technology also offers solutions for data protection, such as encryption, anonymization, and privacy-enhancing technologies. Balancing the benefits of technological innovation with the imperative to protect data privacy remains a central challenge.

3 Data Privacy and Its Issues

Data privacy is not confined by borders; it has global implications. Cross-border data flows, international data transfer agreements and the harmonization of data protection laws are complex issues that require a global perspective. Organizations operating in multiple jurisdictions must navigate a web of diverse regulations, underscoring the need for a unified conceptual framework that respects cultural differences while upholding fundamental data privacy principles.

Major issue arises when the data privacy is breached upon by the other party. Some of the concerns regarding this are as follows:[3]

- Techniques to control what is extracted and to check that data are used for intended purpose.
- Support for both collective security and personal privacy.
- Data privacy policies must be easily understood by the users.
- Users need to be informed about the data sharing/ transfer to the other party.

Furthermore, Data privacy is not merely a legal or technical concern; it is deeply rooted in philosophy, ethics, and the evolving nature of technology. A robust theoretical and conceptual framework for data privacy should balance the rights and autonomy of individuals with the legitimate needs of organizations

[3]Elisa Bertino, "Data Security and Privacy: Concepts, Approaches, and Research Directions**"** in *40th IEEE Annual Computer Software and Applications Conference (COMPSAC 2016)*, Atlanta, GA, June 10–14, 2016, pp 400–407.

and society as a whole. It must also adapt to the dynamic nature of data and technology. As we move forward in the digital age, a comprehensive understanding of data privacy will continue to be essential for crafting effective policies, laws, and ethical standards that protect individuals while fostering innovation and progress.

3.1 Constitutional Precepts

Hon'ble Justice D.Y. Chandrachud in the case of *K.S. Puttaswamy* v. *Union of India*[4] with his concurring opinion emphasized the fundamental nature of the right to privacy as an intrinsic part of the right to life and personal liberty under Article 21 of the Indian Constitution.[5] He observed that privacy is not just a common law right or a statutory right but is inherent in the dignity and integrity of an individual. He further lamented that:

"Privacy is the constitutional core of human dignity. Privacy ensures the fulfilment of dignity".[6]

He has also stressed the need to balance individual privacy with legitimate state interests. He recognized that the state has a legitimate interest in implementing policies for the welfare of the people, but such policies must meet the test of proportionality. He stated that any invasion of privacy must be based on a valid, just, and fair law, and the means employed must be proportional to the ends sought to be achieved.[7] Furthermore, he also underscored that the concept of privacy should evolve with changing times and technologies. He recognized that technological advancements and the digital age pose new challenges to privacy, and the law should adapt to address these challenges.

The Hon'ble Judge delved deeper into the question as to whether the decisions of *M.P. Sharma and ors.* v. *Satish Chandra and Ors.*[8] and *Kharak Singh* v. *Union of India*[9]case needed to be overruled or not. *M.P. Sharma and Ors*. v. *Satish Chandra and Ors.*[10] case was one of the earliest instances where the question of the right to privacy under the Indian Constitution was considered. Through this case it was observed that there was no fundamental right to privacy under the Indian Constitution, and therefore, the search and seizure did not violate any constitutional provisions.

Furthermore, he also had a different perspective on this matter. In his dissenting opinion, he argued that the right to privacy is an essential aspect of personal liberty and is protected under Article 21 of the Indian Constitution, which guarantees the right to life and personal liberty. He suggested that privacy should be recognized as a fundamental right, even though it wasn't the majority opinion at the time. This

[4]2017 (10) SCC 1.
[5]D. D. Basu, *Introduction to the Constitution of India* 121 (Lexis Nexis Publications, 2015).
[6]D. D. Basu, *Introduction to the Constitution of India* 121 (Lexis Nexis Publications, 2015).
[7]*K. S. Puttaswamy* v. *Union of India*, AIR 2017; (2017) 10 SCC 1.
[8]AIR 1954 SC 300.
[9]AIR 1963 SC 1295.
[10]AIR 1954 SC 300.

dissenting view laid the foundation for the eventual recognition of the right to privacy as a fundamental right in the *Puttaswamy case*[11] in 2017.

As far as *Kharak Singh* v. *Union of India*[12] is considered, in this case, the Supreme Court examined the constitutionality of certain police regulations that allowed for surveillance and domiciliary visits of individuals suspected of being involved in criminal activities. The Court, in a divided judgment, upheld some of the regulations but struck down others as unconstitutional. *Maneka Gandhi* v. *Union of India*[13] was a landmark judgment pertaining to constitutional law and individual rights in India which marked a pivotal moment in the evolution of constitutional prudence by redefining the scope and nature of personal liberty guaranteed by the Indian Constitution. Though it does not directly relate with right to privacy but it plays a crucial role in expanding the interpretation of personal liberty under Article 21 of the Constitution of India. It is an essential case that expanded the meaning of personal liberty under the Indian Constitution. This expansion of personal liberty has implications for the right to privacy. The right to live with dignity, as articulated in the judgement, encompasses the right to privacy as part of individual's personal liberty.

4 The Digital Personal Data Protection Act, 2023: An Overview

Privacy as a fundamental right has been recognised by the Universal Declaration Human Right, the International Covenant on Civil and Political Right and in many others International and national treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modern age. The publication of this report reflects the growing importance, diversity and complexity of this fundamental right.[14]

The Digital Personal Data Protection Act, 2023 enacted on August 11, 2023 has become a new reality, in the form of shining new data privacy law. After the enactment, this legislation replaced the relevant provisions of the Information Technology Act, 2000, as amended in 2008 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The object of the Act reads as follows: "An Act 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 term data[15] has been defined as "a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by

[11]*K. S. Puttaswamy* v. *Union of India*, AIR 2017 SC 4161; (2017) 10 SCC 1.
[12]AIR 1963 SC 1295.
[13]AIR 1978 SC 597.
[14]David Banisar and Simon Davies, 'Privacy and Human Rights: An International Survey of Privacy Laws and Developments' 18 *John Marshall Journal of Computer & Information Law* 4 (1999).
[15]The Digital Personal Data Protection Act, 2023, s. 2(h).

automated means." Personal data[16] has been defined as "any data about an individual who is identifiable by or in relation to such data."

Some of the important features of the Act are as follows:

i. Digital Personal Data

The Act applies to the processing of digital personal data, which is broadly defined as data in digital form (whether collected in digital form or in non-digital form and then digitized) about an individual, who is identifiable by such data.

ii. Extra-Territorial Application

The Act applies to the processing of digital personal data in India, and also outside India if such processing is in connection with offering goods or services to data subjects who reside in India.

iii. Obligations of Data Controllers

The Act imposes various obligations on data controllers (or "data fiduciaries" as defined by Act) processing digital personal data of data subjects ("data principals" as defined by Act) in India, including the following:

i. **Consent:** Data controllers require the consent of data subjects in order to process their digital personal data, subject to certain "legitimate use" exceptions (e.g., the voluntary provision of data, to avail of government benefits, in case of medical emergencies, or employment-related data). Such consent should be "free, specific, informed, unconditional and unambiguous" and should be communicated through clear affirmative action signifying agreement to the processing of the data subject's personal data for the specified purpose, and shall be limited to only such personal data as is necessary for such specified purpose. Such consent may also be withdrawn by the data subject.

ii. **Notice:** In order to obtain consent, data controllers should provide the data subjects with a notice specifying what personal data is to be collected, the purposes for which such data will be processed, and how the data subjects can exercise their rights in respect of such data.

iii. **Recordkeeping:** Data controllers will have to demonstrate that notice and consent requirements were met and will need to maintain relevant records.

iv. **Data Transfers:** Digital personal data may be transferred outside of India, except to countries restricted by Indian authorities. The list of restricted countries will be released later by the central government.

v. **Data Breaches:** Data controllers are required to report personal data breaches (which include unauthorized data processing, disclosure, alteration, loss, or actions compromising data

[16]The Digital Personal Data Protection Act, 2023, s. 2(t).

confidentiality, integrity, or availability) to the affected data subjects and to the Data Protection Board of India. The form and manner of such reporting is to be prescribed in rules to be issued by the central government. The reporting obligations under the Act are in addition to the existing reporting obligations under India's Computer Emergency Response Team rules.

vi. **Data of Children and Persons with Disabilities:** Before processing personal data of a child or a person with disabilities who has a lawful guardian, data controllers are required to obtain verifiable consent of the parent or guardian. Certain forms of processing involving children's data (such as online tracking, behavioral/targeted advertising) are strictly prohibited.

vii. **Exemptions:** Data controllers have been granted exemptions, in certain specified circumstances, from specific obligations, such as the requirement for notice and consent. These include instances where the processing of digital personal data is essential for the enforcement of legal rights or claims; processing by Indian courts, tribunals, or other regulatory agencies; processing in the interest of preventing, detecting, investigating or prosecuting offenses or violations of law.

4.1 Rights of Data Subjects

The Digital Personal Data Protection Act of 2023 outlines several rights for data subjects to protect their personal data. These rights generally align with existing data protection regulations such as the GDPR (General Data Protection Regulation) in Europe or similar frameworks in other jurisdictions. Here are some common rights enumerated as follows:

i. **Right to Access:** Data subjects have the right to obtain confirmation from the data controller whether personal data concerning them is being processed and, if so, access to that data.

ii. **Right to Rectification:** Data subjects can request the correction of inaccurate or incomplete personal data.

iii. **Right to Erasure (Right to be Forgotten):** Data subjects have the right to request the deletion of their personal data when it's no longer necessary for the purposes for which it was collected, or if they withdraw consent (where consent is the basis for processing).

iv. **Right to Restriction of Processing:** Data subjects can request the restriction of processing their personal data in certain circumstances, such as when the accuracy of the data is contested.

v. **Right to Data Portability:** Data subjects have the right to receive the personal data they have provided to a controller in a structured, commonly used, and machine-readable format, and to transmit that data to another controller.

vi. **Right to Object:** Data subjects can object to the processing of their personal data in certain situations, such as direct marketing.

vii. **Rights in Relation to Automated Decision Making and Profiling:** Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which produce legal effects concerning them or similarly significantly affect them.

viii. **Right to Lodge a Complaint:** Data subjects have the right to lodge a complaint with a supervisory authority if they believe their rights under the data protection legislation have been infringed.

These rights are designed to give individuals control over their personal data and ensure that their information is handled responsibly by organizations that process it.

4.2 Regulatory Authority

The regulatory authority plays a crucial role in ensuring compliance with data protection principles, handling complaints from data subjects, and imposing sanctions or penalties on organizations that fail to meet their obligations under the law.[17] Here are some key aspects and responsibilities of a regulatory authority in the Act:

i. **Supervision and Enforcement:** The authority would supervise the application of the data protection rules and ensure that organizations comply with the provisions of the act. This includes conducting investigations, audits, and inspections of data controllers and processors.

ii. **Guidance and Advice:** Providing guidance, advice, and interpretation of the data protection laws to organizations and individuals, helping them understand their rights and obligations.

iii. **Handling Complaints:** The regulatory authority would receive and investigate complaints from individuals (data subjects) regarding breaches of their data protection rights. They would have the authority to mediate between parties and take enforcement actions if necessary.

iv. **Issuing Fines and Penalties:** In cases of non-compliance with the data protection regulations, the regulatory authority would have the power to impose fines and penalties on organizations. These penalties are often designed to be proportionate to the severity of the infringement.

v. **Promotion of Awareness:** Promoting public awareness of data protection issues, rights, and best practices through educational campaigns and outreach initiatives.

vi. **International Cooperation:** Collaborating with other data protection authorities internationally, particularly in cases involving cross-border data flows or international data transfers.

vii. **Monitoring Technological Developments:** Keeping abreast of technological advancements and their implications for data protection, and adjusting regulations and guidelines accordingly.

[17]The Digital Personal Data Protection Act, 2023, s. 18(1).

The Regulating authority under Digital Personal Data Protection Act of 2023, plays a crucial role in upholding the principles of transparency, fairness, and accountability in the handling of personal data within the digital realm.

4.3 Penalties

The Digital Personal Data Protection Act, 2023 prescribes penalties for noncompliance of up to 250 crore rupees ($30 million). All the funds realised by the board shall be credited to the consolidated fund of India. Penalties for non-compliance with data protection regulations would typically be structured to ensure that organizations take their obligations seriously and adhere to the principles of data protection. These penalties are essential to deter violations and protect individuals' rights regarding their personal data fund of India.

5 Judicial Interpretation: Global Views

Data privacy is a critical legal and ethical issue in present times and judiciary around the world has delivered judgements in this regard. Some of the notable data privacy judgements are as follows:

5.1 India

Judicial recognition of constitutional protection of privacy right does not in any manner amount to usurpation of legislative function and that sounds true for the magnificent judgement delivered by the Supreme Court of India in the case of Justice *K.S. Puttaswamy* v. *Union of India*[18]. In this case the Supreme Court while deciding the case, referred to the decision in J*ames* v. *Commonwealth of Australia*[19], where in it was observed that, Courts in deciding a particular issue apply different principles, particularly when it comes to the issues of data protection and privacy. In this backdrop, it becomes necessary, while referring to these judgments, to keep in mind the ethos, cultural background and vast socio-economic problems of this country and on that basis to accept a particular norm, or for that matter, to formulate a constitutional norm which is relevant in our case.

In another such case, *Cen. Pub. Information….*v. *Subhash Chandra Aggarwal*[20], wherein the doctrine of the public interest under the RTI Act, turning to examining its co-relation with transparency in the functioning of the judiciary in matters of judicial appointments/selection and importance of judicial independence. The court observed four major arguments are generally invoked to deny third-party or public access to information on appointments/selection of judges, namely, (i) confidentiality concerns; (ii) data protection; (ii) reputation of those being considered in the selection process, especially those whose candidature/eligibility stands negated.

[18]*K. S. Puttaswamy* v. *Union of India*, AIR 2017 SC 4161; (2017) 10 SCC 1.
[19]1936 AC 579.
[20]2019 SCC Online SC 1459.

In yet another case, *Salil Bali* v. *Union of India and another*[21] which relate to position prior to the passing of the new act. The enactment of the Juvenile Justice (Care and Protection of Children) Act, 2000, and the amendments effected thereto in 2006, together with the Rules framed there under in 2007, and the data available with regard to the commission of heinous offences by children, within the meaning of Sections 2(k) and 2(l) of the Juvenile Justice (Care and Protection of Children) Act, 2000, we do not think that any interference is necessary with the provisions of the Statute till such time as sufficient data is available to warrant any change in the provisions of the aforesaid Act and the Rules. On the other hand, the implementation of the various enactments relating to children, would possibly yield better results.

5.2 United States

In *Carpenter* v. *US*[22] court was discussing the issue as to whether the government can access the cell phone records of its peoples. It was finally ruled that government's warrantless collection of cell phone location data violated the Fourth Amendment's protection against unreasonable searches and seizures. The decision recognized that individuals have a reasonable expectation of privacy in their cell phone location data.

In *Lowe's Companies, Inc*. v. *Cook*[23] the Supreme Court declined to review a decision by the Indiana Supreme Court concerning whether customers affected by a data breach had standing to sue the retailer under state law. The state court's decision allowed customers to sue for negligence after their credit card information was stolen in a data breach.

Frank v. *Gaos*[24] involved the settlement of a class action lawsuit against Google over alleged privacy violations. The Supreme Court vacated and remanded the case to lower courts to address concerns about the fairness of the settlement and the plaintiffs' standing to sue.

5.3 European Union

The landmark data privacy case Schrems II[25]has had a significant impact on the digital landscape since it was decided in 2020. The European Court of Justice (ECJ) invalidated the EU-U.S. Privacy Shield agreement in this case, which had allowed the transfer of personal data from the EU to the United States. The judgment emphasized the need for strong data protection standards, particularly in cross-border data transfers.

[21]2013 (7) SCC 705.
[22]138 S. Ct. 2206.
[23]Civil Docket No. 5-:06-2130-RBH.
[24]586 U.S. 2019.
[25] CJEU- C-311/18.(2020).

5.4 Canada

A landmark decision of Supreme Court of Canada *R.* v. *Spensor*[26]throws light on informational privacy. The Supreme Court of Canada ruled that individuals have a reasonable expectation of privacy in their internet subscriber information. This case reinforced the importance of privacy protections in the digital age.

5.5 Australia

In the case of *Privacy Commissioner* v. *Telstra Corporation Ltd*[27] the Australian Federal Court held that metadata should be considered personal information. The judgment clarified the legal status of metadata and its protection under Australian privacy laws. The judgment clarified the legal status of metadata and its protection under Australian privacy laws.

These judgments reflect the evolving legal landscape surrounding data privacy and the recognition of privacy as a fundamental right in many jurisdictions. They have played a crucial role in shaping data protection laws and practices around the world.

6 Conclusion and Suggestions

Thus, one could conclude that the Digital Personal Data Protection Act of 2023 represents a significant milestone in safeguarding the privacy of individuals in the digital age. As we navigate an increasingly interconnected and data-driven world, the need for comprehensive data protection measures has never been more critical. This legislation not only recognizes the value of personal data but also establishes a robust framework to ensure its secure handling, storage, and processing.

The Act emphasizes transparency, accountability, and consent as fundamental principles, empowering individuals to have more control over their personal data. It sets strict guidelines for data collectors, processors, and controllers, compelling them to adhere to stringent security standards and report data breaches promptly.

Additionally, the Act encourages the development and adoption of privacy-enhancing technologies, ensuring that data protection evolves alongside technological advancements. It also represents a significant step towards ensuring the privacy and security of digital data in an increasingly interconnected world. This legislation aims to address the evolving challenges of data protection by implementing robust measures to safeguard personal information.

Crucially, the Act also incorporates provisions to address emerging challenges such as cross-border data transfers and the protection of sensitive information, ensuring that privacy remains at the forefront of

[26]2014 SCC 43.
[27](2017) FCAFC 4.

digital innovation. By placing individuals' rights and interests at its core, this legislation strikes a balance between fostering innovation and safeguarding data privacy.

As we move forward into the digital era, the Digital Personal Data Protection Act of 2023 serves as a vital framework for protecting individuals' rights and fostering trust in the digital ecosystem. It underscores the importance of data privacy as a fundamental human right and paves the way for a more secure, responsible, and ethically driven digital landscape. However, its effective implementation, ongoing enforcement, and adaptation to evolving technological landscapes will be essential to ensure the enduring protection of personal data and the preservation of individual privacy in the years to come.

****