INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ANALYSIS OF LEGAL FRAMEWORK GOVERNING DATA PRIVACY IN INDIA

AUTHORED BY - KANISHK SHUKLA

1.Introduction

From a country of Vedas and manuscripts to the country, which is leading in the IT sector, being placed among top 6 global hub[1] worldwide. Now we live in an era where day to day activity from social media and mobile apps to online transactions and government services has made our life so interconnected with modern technology that it amounts to 'need' of an individual and not being affected by its influence feels unimaginable. The drive of need has led human civilization to achieve wonders one of the prime example can be stated as Technological advancements which in turn has helped human race in bringing rapid change in the society at large through its invention in various fields like health sector, communication sector, banking so on. The 21st century has brought a new wave of revolution in the field of technology which is commonly expressed as digital revolution and India is no exception to the cause whilst placing itself in 14th position in Global Startup Ecosystem Report (GSER) in 2025[2]. In India not only urban population is highly indulged in internet usage but we can also find the rural population to be equally participating in the revolution. With the extension in accessibility, we are seeing a world where communication and information sharing is easy, making privacy sensitive to vulnerabilities. Traditionally, privacy was understood in a physical sense such as, privacy of one's home, correspondence, and bodily integrity. In the digital age, however, privacy has expanded to include informational self-determination, meaning the right of individuals to control how their personal data is collected, processed, stored, and shared. Looking into this government of India recently implemented "Digital India" drive which resulted in processing of large number of personal data which resulted in mixed blessing as it rendered many advantages but has also put our right to privacy at risk. The public and private sector currently are heavily indulged in amassing personal data carelessly as excessive amount of people are using internet for their daily life activities and constantly uploading their personal information in various apps and forms. For example: when people file forms for colleges, Government or private exams or data input for online marketing or shopping; posts on social

[1] Facebook/CMofKarnataka/MBPatilMLA
[2] https://www.angelone.in/news/market-updates

ISSN: 2582-6433

media; uploading Curriculum Vitae in various job sites; buying sim cards or phone connections; not only adults but children's also click on links in their games, etc. All these activities need us to put our major personal information's like the full name, address, contact details, location, etc. All these information's which though seem as been put by an individual with his/her consent only for specific purposes but can also be accessed by the hackers, rural population being heavily indulged in internet usage are more prone to be affected by attacks from hackers and advertisement organization as they are not fully able to understand the term of service and the consequences which may fall upon them. This screams for the laws for protection of data and protection of constitutional right, specifically, vested under Articles 19(1)(a) and 21 of the Constitution of India.

Historically, data protection in India was governed by the Information Technology Act, 2000, which primarily focused on electronic commerce and cybersecurity[3]. While the Act included certain provisions related to data protection, such as Section 43A dealing with compensation for failure to protect data, it was not designed to address the complexities of modern data-driven technologies. The subsequent introduction of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 sought to fill some of these gaps by defining sensitive personal data and imposing obligations on body corporates[4]. However, these rules were limited in scope and lacked comprehensive enforcement mechanisms. It was until 2023 that India did not have a standalone law or framework to govern data protection and only after releasing different draft versions of a data protection legislation and considering the recommendations from different stakeholders, the Ministry of Electronics and Information Technology, Government of India, released the draft of the Digital Personal Data Protection Bill in 2022 (DPDP Bill) which introduced an statute to strengthen the data protection law of the country.

A transformative development in the Indian legal landscape occurred with the landmark judgment of the Supreme Court in Justice K.S. Puttaswamy v. Union of India[5]. In this case, a nine-judge bench unanimously recognized the right to privacy as a fundamental right under Article 21 of the Constitution. The judgment emphasized that privacy is intrinsic to human dignity and liberty and must be protected against arbitrary state action as well as non-state

[3] Information Technology Act, 2000 (Act 21 of 2000).
[4] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[5] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

ISSN: 2582-6433

actors. This decision not only reinforced constitutional protections but also highlighted the urgent need for a comprehensive data protection regime in India.

Following this judgment, the Government of India constituted a committee of experts under the chairmanship of Justice B.N. Srikrishna to examine issues related to data protection and recommend a suitable legal framework. The committee's report laid the foundation for subsequent legislative efforts and emphasized principles such as consent, purpose limitation, data minimization, and accountability[6].

In response to these developments, the Indian legislature enacted the Digital Personal Data Protection Act, 2023, marking a significant step toward establishing a comprehensive data protection framework[7]. The Act seeks to regulate the processing of digital personal data, ensure that individuals have control over their data, and impose obligations on entities handling such data. It introduces key concepts such as data fiduciaries, data principals, and consent-based processing, thereby aligning India's legal framework with global standards to a certain extent. Despite these advancements, concerns remain regarding the adequacy and effectiveness of India's data protection regime. Issues such as enforcement challenges, lack of awareness, and the evolving nature of technology continue to pose significant obstacles. Therefore, a critical examination of the legal framework governing data privacy in India is both timely and necessary.

1.2 Objectives of the Study

The primary objectives of this study are as follows:

- To examine the concept and significance of data privacy in the digital era
- To analyze the evolution of data protection laws in India
- To study the provisions of the Digital Personal Data Protection Act, 2023
- To evaluate the impact of judicial decisions, particularly Justice K.S. Puttaswamy v. Union of India
- To identify challenges in the implementation of data privacy laws
- To suggest reforms for strengthening the legal framework

[6] Ministry of Electronics and Information Technology, Government of India, *Report of the Committee of Experts on Data Protection (Srikrishna Committee Report)*, 2018.
[7] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

ISSN: 2582-6433

1.3 Research Questions

This study is guided by the following research questions:

1. What is the scope and meaning of data privacy in the digital age?
2. How has the legal framework for data protection evolved in India?
3. What are the key features of the Digital Personal Data Protection Act, 2023?
4. How effective are current laws in protecting personal data?
5. What challenges exist in the enforcement of data privacy laws in India?

1.4 Research Methodology

This research adopts an analytical methodology, focusing on the study of legal texts, judicial decisions, and scholarly literature. The research is qualitative in nature and relies on both primary and secondary sources.

Primary sources include statutes such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, as well as judicial pronouncements including Justice K.S. Puttaswamy v. Union of India[8]. Secondary sources include books, journal articles, committee reports, and online legal databases.

The research employs methods such as legal interpretation, comparative analysis, and critical evaluation to analyze the effectiveness of the legal framework.

1.5 Scope of the Study

The study focuses on current condition of the legal framework governing data privacy and data protection in India, with emphasis on the Digital Personal Data Protection Act, 2023 and Information Technology Act, 2000. It also incorporates a limited comparative perspective to understand global best practices and identify gaps in the Indian framework.

1.6 Significance of the Study

The significance of this study lies in its attempt to critically analyze the legal framework governing data privacy in India. By identifying gaps and challenges, the research aims to contribute to the ongoing discourse on data protection and provide recommendations for strengthening the legal regime.

[8] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

ISSN: 2582-6433

2. Concept of Data Privacy and Data Protection

The modern India is embracing digitalization with full support from its rural and urban population, in digital India we come across the words like "data privacy" and "data protection" which are well-known in the public and legislative spheres. The majority population of digital India have become a more tech-savvy population because of which an increasing number of businesses are executing digital operations, leading to large volume of personal data being collected, processed, and stored. This has led us to concern ourselves that how our data is collected and how it is protected from abuse and illegal access. This concern can be dealt by understanding the concept of "data privacy" and "data protection" and its application on Indian laws.

Though the phrases "data privacy" and "data protection" are sometimes used interchangeably, they have distinct legal and operational definitions. The main focus of data privacy is on an individual's right to control who can access and use their personal information. Data protection, on the other hand, centres on the security measures an entity uses on its legal, administrative, and technical measures to safeguard such data from misuse. The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India[9] has further strengthened the importance of these concepts in the Indian legal framework.

2.2 Meaning and Concept of Data Privacy

The introduction of digital technologies has brought about a drastic change in the concept of data privacy such as sensitive digital footprints. In the past, people thought of privacy in physical terms, such as privacy of one's home, correspondence, and physical safety. Nevertheless, in the digital era, privacy has broadened to include informational self-determination, which is the right of individuals to manage how their personal data is gathered, processed, stored, and distributed.

Data privacy refers to the right of individuals to control the collection, use, and dissemination of their personal information. It ensures that individuals are informed about how their data is collected and used, and that such use is subject to their consent.

Personal data includes any information that can identify an individual, either directly or indirectly. This includes names, contact details, identification numbers, financial information, and digital identifiers.

[9] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

ISSN: 2582-6433

The Digital Personal Data Protection Act, 2023 defines personal data as any data about an individual who is identifiable by or in relation to such data[10]. The Act establishes a consent-based framework, emphasizing the rights of individuals, referred to as "data principals."

Data privacy is essential for protecting individual autonomy, dignity, and freedom in the digital environment.

2.3 Meaning and Concept of Data Protection

Data protection refers to the mechanisms and legal frameworks designed to safeguard personal data from unauthorized access, misuse, or disclosure. It includes policies, procedures, and technologies that ensure data security and compliance with legal standards.

Unlike data privacy, which is concerned with individual rights, data protection focuses on the responsibilities of organizations and governments in handling data. It involves measures such as encryption, access controls, data minimization, and secure storage.

In India, data protection has evolved through legislative measures such as the Information Technology Act, 2000[11] and the Digital Personal Data Protection Act, 2023[12]. These laws impose obligations on entities handling personal data and provide remedies in case of data breaches.

2.4 Distinction between Data Privacy and Data Protection

Though they are often used interchangeably, data protection and data privacy are clearly different in their scope and use.

- Meaning:

  Data privacy deals with the rights that individuals have over their own data. Data Protection, though, stresses the techniques used to secure that data. Data protection is a legal and regulatory system for upholding privacy, which is a basic right.
- Nature:

  Data privacy has a moral and legal character; data protection concentrates on the technical and procedural elements.
- Goal:

  Data Privacy guarantees the right handling of personal data, while Data Protection protects against unlawful access or breaches.

[10] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
[11] Information Technology Act, 2000 (Act 21 of 2000).
[12] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

ISSN: 2582-6433

- For example:

  Data protection ensures encryption of data and application of cyber security technologies, whereas data privacy ensures user permission.

2.5 Evolution of Privacy and Data Protection

The concept of privacy is articulated in human beings through their indulgence in societal norms and ethics still the evolution of civilisation and rapid growth towards digital era has left a blank space where the expert such as hackers use it for satisfying their greed. This act is not left unnoticed, but until 2023 there was no concrete framework to safeguard the masses digital privacy as the understanding towards privacy was not properly laid down under the then rules mentioned under Information Technology Act 2000 and Information Technology Rules 2011, though it took sometime to governing bodies to provide society with proper statutory protection but it was finally evolved from a narrow understanding of physical privacy to a broader notion of informational privacy and reached a significant turning point in the administration of justice with Justice K.S. Puttaswamy v. Union of India, where the Supreme Court recognized privacy as a fundamental right under Article 21[13]. This judgement broadened horizon of law makers and they drafted different versions of legislations for strengthening data protection and privacy framework for India. The Ministry of Electronics and Information Technology (MeitY), Government of India, published the draft of the Digital Personal Data Protection Bill (DPDP Bill) in 2022 after releasing several draft versions of data protection law and taking into account feedback from various parties. The DPDP Bill, as it was ultimately approved by both chambers of the Indian Parliament, included a few notable modifications to the original text. The Digital Personal Data Protection Act, 2023 (DPDP Act), which will establish India's regulatory and personal data protection framework, was released by the Indian government on August 11, 2023. The DPDP Act establishes a number of regulations governing the acquisition, processing, storage, and exchange of digital personal information. The MeitY announced the DPDP Act and the Digital Personal Data Protection Rules, 2025 (DPDP Rules) on November 13, 2025. In a phased manner, certain portions of the DPDP Act and the regulations established under the DPDP Rules will take effect.

Globally, data protection frameworks such as EU's General Data Protection Regulation (GDPR) has greatly influenced the DPDP Act but the act requires further refinements to meet India’s unique socio-political needs[14]. These frameworks greatly emphasize accountability,

[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[14] European Union, General Data Protection Regulation (EU) 2016/679.

ISSN: 2582-6433

transparency, and individual rights.

2.6 Principles of Data Privacy and Data Protection

To tackle with the modern problems data protection laws are based on certain key principles:

- **Consent:** Under the DPDP Act, consent is necessary for the processing of personal data. The GDPR's guiding principles require that consent be unambiguous, express, and well-informed. In addition, individuals have the right to revoke their permission at any time, and data fiduciaries are obligated to ensure that data is deleted upon withdrawal, unless there are overriding legal obligations
- **Purpose Limitation:** The data may only be used for the purposes stated at the time of acquisition. The DPDP Act limits the usage and repurposing of data without the subject's agreement by prohibiting "bundled consent" methods and mandating that consent be given separately for each purpose.
- **Data Minimization:** The DPDP Act mandates that businesses only collect the information necessary for the stated objective and guarantee its safety. This idea, which is consistent with data protection legislation, requires companies to employ stringent security measures to avoid breaches and unauthorized access.
- **Privacy in Social Media:** Social media companies are known to gather enormous volumes of user data through profiling, which raises privacy issues. In this case, platforms are required under data privacy standards to acquire express consent before collecting personal data, particularly for behavioral or targeted advertising. Users' rights to know how their data is used and to seek its erasure are upheld under the DPDP Act.
- **Accountability:** Organizations must be responsible for data handling. This principle lays great emphasis to banking sector as large amount of private data is dealt by the bank so banks must protect their clients' personal and financial information from unwanted access. Banking information must be protected using data protection procedures including secure access restrictions, encryption, and frequent vulnerability assessments. These procedures emphasize data security, guaranteeing the confidentiality and integrity of information inside the company.
- **Transparency:** Clear information must be provided to users and this principle also concerns itself with cross border transfer of data the federal government can impose restrictions on cross-border data transfers under the DPDP Act. In order to shield residents' data from exposure in countries with insufficient protection measures, the Act provides for the blacklisting of certain locations, even if it usually authorizes data

ISSN: 2582-6433

transfers. This is vital for maintaining compliance with international norms and preserving Indian citizens' data.

These principles are reflected in both the Digital Personal Data Protection Act, 2023 and the General Data Protection Regulation[15].

2.7 Importance of Data Privacy and Data Protection

The importance of data privacy and data protection can be understood as follows:

- **Protection of Fundamental Rights:** Ensures dignity and liberty of individuals
- **Prevention of Cybercrime:** Reduces risks of identity theft and fraud
- **Trust in Digital Economy:** Encourages user confidence in online systems
- **Regulation of Corporate Practices:** Ensures accountability of organizations

The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India reinforces the need for strong data protection measures[16].

2.8 Conclusion

Data privacy and data protection are essential components of the modern digital ecosystem. While data privacy focuses on individual rights, data protection provides the framework to enforce those rights. The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India and the enactment of the Digital Personal Data Protection Act, 2023 represent significant steps in strengthening India's legal framework.

However, effective implementation, public awareness, and continuous adaptation to technological advancements are crucial to ensuring robust protection of personal data.

3. The Right to Privacy's Constitutional Basis

3.1 Historical Jurisprudence on Privacy

For many years, there was debate about the constitutional status of the right to privacy in India. Among the basic rights listed in Part III, the Indian Constitution of 1950 does not specifically mention the right to privacy. The lack of textual silence in this area resulted in conflicting legal viewpoints about whether privacy might be inferred from other constitutional clauses.

In M.P. Sharma v. Satish Chandra, the first important statement on privacy was made. An eight-judge Bench of the Supreme Court refused to acknowledge a right to privacy comparable to the Fourth Amendment's safeguard against unreasonable searches and seizures in the United

[15] Digital Personal Data Protection Act, 2023; General Data Protection Regulation (EU) 2016/679.
[16] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

ISSN: 2582-6433

States Constitution. The Indian Constitution does not include a clause similar to the Fourth Amendment, according to the Court, hence the right to search and seize cannot be contested on the basis of privacy.

The Supreme Court reaffirmed this tight stance in Kharak Singh v. State of U.P., where a six-judge bench debated the constitutionality of specific rules governing police surveillance. In his dissenting view, Justice Subba Rao presented a larger view of personal freedom under Article 21 that included the right to privacy, even if the majority opinion held that the Indian Constitution did not have a basic right to privacy. He noted that the right to individual liberty "is not merely freedom from physical restraint or freedom from confinement within the bounds of a prison, but something more."

Despite this disagreement, the majority opinion in Kharak Singh still casts a long shadow over privacy law in India. Later judgments, though, started to acknowledge privacy in certain situations while leaving its constitutional position unclear. In Gobind v. State of M.P., Justice Mathew, writing for a three-judge Bench, assumed but did not decide that the right to life and personal liberty included a right to privacy, even if that right was not absolute and could be limited.

3.2 The Puttaswamy Judgment: Privacy Is a Fundamental Right

The nine-judge Constitution Bench's ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India[17], which was a watershed moment in Indian constitutional law, definitively established the constitutional status of privacy. The dispute stemmed from objections to the Aadhaar system, which required a preliminary decision on whether the right to privacy is a fundamental right guaranteed by the Constitution.

The Supreme Court unanimously decided that the right to privacy is a basic right protected by Part III of the Constitution, particularly by Article 21, which ensures the right to life and personal freedom. To the extent that the majority decisions in M.P. Sharma and Kharak Singh held that there was no basic right to privacy, the Court overturned them.

Writing the majority opinion on behalf of himself and three other judges, Justice D.Y. Chandrachud expressed a three-dimensional understanding of privacy[18] that included:

1. Privacy of the individual (physical or bodily privacy)
2. informational privacy (protection of personal data and information)
3. The freedom to make your own decisions about your life (privacy of choice).

[17] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[18] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

ISSN: 2582-6433

Justice Chandrachud made the following remarks on informational privacy, which is the aspect of data protection that is most directly related to data protection:

"The right to privacy includes informational privacy as one of its aspects. In an era of information, threats to privacy might come from non-state entities in addition to the government. We urge the Union Government to investigate and establish a strong data protection system.

The Court acknowledged that data about people may reveal private facts about their lives, tastes, relationships, and views in the digital age. The collection, storage, and processing of such data by both public and commercial organizations poses a serious threat to people's independence and dignity. As a result, the court established the constitutional basis for laws providing complete data protection.

3.3 The Proportionality Test

One of the most important aspects of the Puttaswamy decision was its articulation of a proportionality standard for determining limits on the right to privacy. Any violation of privacy must meet the following criteria, according to the Court:

1. Legality: It must be required by law.
2. Legitimate goal: Legitimate state interests must be prioritized by the law.
3. Proportionality: The limitation must be proportionate to the requirement and must be the least restrictive method of accomplishing the stated goal.
4. procedural protections: The law must include safeguards against abuse.

Data protection law is greatly impacted by this proportionality framework. Any state collection, processing, or storage of personal information must be legally permitted, must have a legitimate purpose, must be restricted to what is essential to accomplish that objective, and must be protected against misuse.

3.4 Developments After Puttaswamy

In later cases, most notably Justice K.S. Puttaswamy (Retd.) v. Union of India (the Aadhaar case), where a five-judge Constitution Bench considered the constitutional validity of the Aadhaar scheme and the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, the principles enunciated in the first Puttaswamy judgment were used.

Although the majority of the laws supported the fundamental Aadhaar framework, they repealed numerous clauses that did not adhere to the proportionality requirement. Notably,

ISSN: 2582-6433

Section 57 of the Aadhaar Act, which permitted the use of Aadhaar authentication by private organizations, was repealed. The Court decided that forcing people to provide private companies with their biometric information in order to use their services was an excessive infringement on informational privacy and lacked a valid governmental objective.

The Aadhaar decision highlighted the necessity for thorough data protection legislation that would govern how personal information is collected and used by both public and private parties[19]. The Digital Personal Data Protection Act of 2023 was enacted with additional constitutional support as a result.

Srikrishna Committee Report, 2018

In response to the need for a comprehensive data protection framework, the Government of India constituted a committee under Justice B.N. Srikrishna. The committee submitted its report in 2018, recommending the introduction of a dedicated data protection law.

The report proposed key principles such as:

- Consent-based data processing
- Data minimization
- Purpose limitation
- Accountability of data fiduciaries

The committee also emphasized the importance of balancing individual privacy with the interests of the state and businesses.

4. The Information Technology Act, 2000 and Related Rules

4.1 Overview of the IT Act, 2000

The Information Technology Act, 2000, enacted to provide legal recognition for electronic transactions and facilitate e-commerce, contains provisions relevant to data protection, though it was not designed as a comprehensive data protection statute[20]. The Act underwent significant amendments in 2008, which introduced provisions specifically addressing data protection and cyber security.

Section 43A of the IT Act, inserted by the 2008 amendment, imposes liability on body corporates possessing, dealing, or handling sensitive personal data or information in a computer resource, where such body corporate is negligent in implementing and maintaining reasonable security practices and procedures, thereby causing wrongful loss or wrongful gain to any person. The provision enables compensation for individuals who suffer damage as a result of

[19] K.S. Puttaswamy (Aadhaar) v. Union of India, (2019) 1 SCC 1.
[20] Information Technology Act, 2000 (Act 21 of 2000).

ISSN: 2582-6433

such negligence.

Section 72 of the IT Act provides penalties for breach of confidentiality and privacy. It prescribes punishment for any person who, in pursuance of powers conferred under the Act, rules, or regulations, has secured access to any electronic record, book, register, correspondence, information, document, or other material and discloses such information without the consent of the person concerned.

Section 72A, inserted by the 2008 amendment, addresses the disclosure of information in breach of lawful contract. It penalizes intermediaries and persons who, while providing services under a lawful contract, have secured access to personal information about another person and disclose such information with the intent to cause or knowing that disclosure is likely to cause wrongful loss or wrongful gain.

4.2 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), issued under Section 43A of the IT Act, constituted India's primary regulatory framework for data protection[21] prior to the enactment of the Digital Personal Data Protection Act, 2023.

4.2.1 Scope and Definitions

The SPDI Rules apply to body corporates or persons located in India that collect, receive, possess, store, deal, or handle information of providers of information residing in India or outside India. The Rules introduce the concept of "sensitive personal data or information" (SPDI), which is defined to include:

- Passwords
- Financial information such as bank account, credit card, debit card, or other payment instrument details
- Physical, physiological, and mental health conditions
- Sexual orientation
- Medical records and history
- Biometric information

The Rules distinguish between "personal information," defined as any information that relates to a natural person capable of identifying such person, and SPDI, which receives higher levels

[21] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

ISSN: 2582-6433

of protection.

4.2.2 Key Obligations

The SPDI Rules impose several obligations on body corporates handling personal information and SPDI:

Privacy Policy: Rule 4 requires body corporates to provide a privacy policy for handling or dealing in personal information, including SPDI. The policy must be published on the website and must contain clear disclosures regarding the type of information collected, the purpose of collection, disclosure practices, and security practices.

Consent: Rule 5(1) mandates that body corporates collecting SPDI must obtain consent in writing through letter, fax, or email from the provider of information regarding the purpose of usage before collecting such information.

Purpose Limitation: Under Rule 5(3), body corporates are prohibited from collecting SPDI unless it is collected for a lawful purpose connected with a function or activity of the body corporate, and the collection is necessary for that purpose.

Disclosure Restrictions: Rule 6 restricts the disclosure of SPDI to third parties without prior permission of the provider of information, subject to exceptions for legal obligations, contractual requirements, and specific regulatory requirements.

Transfer of Information: Rule 7 permits the transfer of SPDI to any body corporate or person in India or outside India that ensures the same level of data protection as provided under the Rules. Transfer is permitted where necessary for the performance of a lawful contract or where the provider has consented to such transfer.

Security Practices: Rule 8 requires body corporates to implement reasonable security practices and procedures, which are deemed satisfied where the body corporate has implemented security practices and standards as certified by an independent auditor, including compliance with IS/ISO/IEC 27001 or codes of best practices approved by the Central Government[22].

4.2.3 Limitations of the SPDI Rules

While the SPDI Rules represented an important step in data protection regulation, they suffered from several limitations that became increasingly apparent as India's digital economy expanded:

1. **Limited Scope:** The Rules applied only to body corporates, leaving government departments and agencies outside their purview. This was particularly problematic

[22] Ministry of Communications and Information Technology, Government of India, *The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*, G.S.R. 313(E), dated 11 April 2011.

ISSN: 2582-6433

given the vast amounts of personal data collected by the state through schemes like Aadhaar.

2. **Narrow Definition of SPDI**: The definition of SPDI, while covering certain categories, did not encompass all types of sensitive information. Notably, information such as caste, religion, political opinions, and genetic data were not included.
3. **Inadequate Enforcement**: The Rules lacked an independent supervisory authority with powers to investigate complaints, conduct audits, and impose penalties. Enforcement relied primarily on civil litigation.
4. **Consent-Centric Approach**: The Rules heavily emphasized consent without adequate recognition of the limitations of consent in the digital age, where privacy policies are lengthy, complex, and rarely read.
5. **Cross-Border Transfers**: The provisions on cross-border data transfers lacked clarity and did not provide mechanisms for assessing the adequacy of protection in recipient jurisdictions.

4.3 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021), issued under Sections 69A and 79 of the IT Act[23], contain provisions relevant to data protection, particularly regarding intermediaries.

Rule 3(1)(a) requires intermediaries to inform users about the rules and regulations, privacy policy, and user agreement before providing access to computer resources. Intermediaries must inform users not to host, display, upload, modify, publish, transmit, store, update, or share information that belongs to another person without authorization or violates privacy.

Significantly, Rule 4(2) requires significant social media intermediaries (defined as intermediaries with five million or more registered users in India) to enable traceability of the originator of information on their platforms when required by a court order or government order. This provision has raised substantial privacy concerns regarding the potential for weakening end-to-end encryption and enabling surveillance[24].

The IT Rules, 2021, also impose obligations on publishers of news and current affairs content and publishers of online curated content, requiring them to observe the principles of self-

[23] Information Technology Act, 2000 (Act 21 of 2000), s.69A and s.79.
[24] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

ISSN: 2582-6433

regulation, including those relating to the collection and use of personal data.

5. The Digital Personal Data Protection Act, 2023

5.1 Legislative Background and Development

The enactment of comprehensive data protection legislation in India followed a prolonged deliberative process spanning several years. The *Puttaswamy* judgment in 2017 provided the constitutional mandate for such legislation, with the Court expressly recommending that the government establish a robust data protection regime.

In August 2017, the Ministry of Electronics and Information Technology constituted a Committee of Experts under the chairmanship of Justice B.N. Srikrishna to study various issues relating to data protection and recommend a draft data protection bill. The Committee submitted its report titled "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians" along with the draft Personal Data Protection Bill in July 2018.

The Personal Data Protection Bill, 2019, introduced in Parliament, underwent extensive examination by a Joint Parliamentary Committee, which submitted its report in December 2021. The Bill was subsequently withdrawn in August 2022, and a revised draft—the Digital Personal Data Protection Bill, 2022—was released for public consultation. Following further revisions, the Digital Personal Data Protection Bill, 2023, was introduced in Parliament and received Presidential assent on 11 August 2023, becoming the Digital Personal Data Protection Act, 2023 (DPDP Act).

5.2 Key Definitions and Concepts

The DPDP Act introduces several key definitions that form the conceptual foundation of the statutory framework:

Data: Section 2(h) defines "data" as 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.

Digital Personal Data: Section 2(n) defines "digital personal data" as personal data in digital form. The Act applies only to digital personal data.

Personal Data: Section 2(t) defines "personal data" as any data about an individual who is identifiable by or in relation to such data.

Data Principal: Section 2(j) defines "data principal" as the individual to whom the personal data relates. Where the individual is a child, the term includes the parent or lawful guardian. Where the individual is a person with disability, it includes the lawful guardian acting on their

ISSN: 2582-6433

behalf.

Data Fiduciary: Section 2(i) defines "data fiduciary" as any person who, alone or in conjunction with other persons, determines the purpose and means of processing personal data.

Data Processor: Section 2(k) defines "data processor" as any person who processes personal data on behalf of a data fiduciary.

Processing: Section 2(x) defines "processing" in relation to personal data as meaning a wholly or partly automated operation or set of operations performed on digital personal data, including collection, recording, organization, structuring, storage, adaptation, retrieval, use, alignment, combination, indexing, sharing, disclosure, restriction, erasure, or destruction.

Consent Manager: Section 2(g) defines "consent manager" as a person registered with the Data Protection Board who acts as a single point of contact to enable data principals to give, manage, review, and withdraw consent through an accessible, transparent, and interoperable platform.

5.3 Applicability and Territorial Scope

Section 3 of the DPDP Act defines its applicability. The Act applies to:

1. Processing of digital personal data within the territory of India, where such data is:
    - Collected online; or
    - Collected offline and subsequently digitized.
2. Processing of digital personal data outside India, where such processing is in connection with any activity related to offering goods or services to data principals within India.

The Act thus has extraterritorial application to foreign entities that process personal data of individuals in India in connection with offering goods or services to them, similar to the approach adopted by the European Union's General Data Protection Regulation (GDPR)[25].

Section 3(c) enumerates exemptions from the Act's application, including:

- Personal data processed by an individual for personal or domestic purposes
- Personal data made publicly available by the data principal or any other person who is under an obligation under any law to make such data publicly available

5.4 Grounds for Processing Personal Data

Chapter II of the DPDP Act establishes the grounds for lawful processing of personal data.

5.4.1 Consent

Section 6 provides that a person may process personal data of a data principal only in

[25] Digital Personal Data Protection Act, 2023; General Data Protection Regulation (EU) 2016/679.

ISSN: 2582-6433

accordance with the provisions of the Act and for a lawful purpose:

1. For which the data principal has given consent; or
2. For certain legitimate uses specified in Section 7.

Section 6(2) sets out the requirements for valid consent. Consent must be:

- Free
- Specific
- Informed
- Unconditional
- Unambiguous
- Given by clear affirmative action
- Signifying agreement to the processing of personal data for the specified purpose

The consent must be limited to the personal data necessary for the specified purpose.

Section 6(6) imposes specific requirements regarding the clarity and accessibility of requests for consent[26]. Every request for consent must be presented in a clear and plain language, specifying the personal data to be collected, the purpose of processing, and the manner in which the data principal may exercise their rights.

5.4.2 Legitimate Uses

Section 7 specifies certain "legitimate uses" for which personal data may be processed without consent:

1. Where the data principal voluntarily provides personal data and it is reasonably expected that such data will be processed.
2. Processing by the State or any instrumentality of the State for:
    - Any function under any law
    - Provision of any service, benefit, subsidy, certificate, license, or permit
3. Processing for compliance with any judgment, decree, or order of any court or tribunal.
4. Processing for responding to a medical emergency involving a threat to the life or immediate threat to the health of the data principal or any other individual.
5. Processing for taking measures during any disaster or breakdown of public order, to ensure safety of any individual or provide assistance or services.
6. Processing for employment purposes, including prevention of corporate espionage, maintenance of confidentiality, recruitment, termination, and provision of services to employees.

[26] Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s.6(6).

ISSN: 2582-6433

5.5 Obligations of Data Fiduciaries

Chapter II also establishes the obligations of data fiduciaries.

5.5.1 General Obligations

Section 8 imposes several general obligations on data fiduciaries[27]:

Compliance: Data fiduciaries must comply with the provisions of the Act regardless of any failure by the data principal to perform their duties.

Purpose Limitation: Processing must be only for the purpose for which consent was given or for which it constitutes a legitimate use.

Data Minimization: Data fiduciaries shall not collect personal data beyond what is necessary for the specified purpose.

Accuracy: Data fiduciaries must make reasonable efforts to ensure that personal data is accurate and complete, particularly where it is to be used to make a decision affecting the data principal or disclosed to another data fiduciary.

Retention Limitation: Data fiduciaries must not retain personal data beyond the period necessary for the specified purpose, unless retention is required by law. Upon the purpose being fulfilled or consent being withdrawn, and in the absence of any legal requirement for retention, the data fiduciary must erase the personal data.

Security: Data fiduciaries must implement appropriate technical and organizational measures to ensure effective observance of the Act, including implementing reasonable security safeguards to prevent personal data breaches.

Breach Notification: Section 8(6) requires data fiduciaries to notify the Data Protection Board and affected data principals of any personal data breach in the prescribed manner.

Grievance Redressal: Data fiduciaries must publish the business contact information of a Data Protection Officer or person responsible for grievance redressal and must respond to grievances within the prescribed time period.

5.5.2 Additional Obligations for Significant Data Fiduciaries

Section 10 empowers the Central Government to notify any data fiduciary or class of data fiduciaries[28] as "Significant Data Fiduciaries" based on factors including:

- Volume and sensitivity of personal data processed
- Risk to the rights of data principals
- Potential impact on sovereignty and integrity of India
- Risk to electoral democracy

[27] Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s.8.
[28] Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s,10.

ISSN: 2582-6433

- Security of the State
- Public order

Significant Data Fiduciaries are subject to additional obligations under Section 10(2):

1. Appointment of a Data Protection Officer based in India who represents the Significant Data Fiduciary
2. Appointment of an independent data auditor to carry out data audits
3. Undertaking Data Protection Impact Assessments
4. Periodic audits by an independent data auditor
5. Such other measures as may be prescribed

5.6 Rights of Data Principals

Chapter III of the DPDP Act confers rights upon data principals.

5.6.1 Right to Access Information

Section 11 grants data principals the right to obtain from a data fiduciary:

1. A summary of personal data being processed and the processing activities undertaken
2. The identities of all other data fiduciaries and data processors with whom personal data has been shared, along with a description of the shared data

5.6.2 Right to Correction and Erasure

Section 12 provides data principals with the right to:

1. Correction of inaccurate or misleading personal data
2. Completion of incomplete personal data
3. Updating of personal data
4. Erasure of personal data that is no longer necessary for the purpose for which it was processed, unless retention is required by law

5.6.3 Right of Grievance Redressal

Section 13 establishes the right of data principals to have readily available means of grievance redressal provided by the data fiduciary. Data principals may also make complaints to the Data Protection Board.

5.6.4 Right to Nominate

Section 14 grants data principals the right to nominate any other individual who shall, in the event of death or incapacity of the data principal, exercise the rights of the data principal.

5.7 Special Provisions for Children and Persons with Disabilities

Section 9 establishes specific protections for children (defined as individuals below eighteen

ISSN: 2582-6433

years of age) and persons with disabilities who have lawful guardians[29]:

1. Data fiduciaries must obtain verifiable consent of the parent or lawful guardian before processing personal data of a child or person with disability.
2. Data fiduciaries shall not undertake tracking, behavioral monitoring, or targeted advertising directed at children.
3. Data fiduciaries shall not undertake any processing of personal data that is likely to cause any detrimental effect on the well-being of a child.

The Central Government may exempt certain data fiduciaries or classes of data fiduciaries from these requirements, having regard to the volume and nature of personal data processed.

5.8 Cross-Border Data Transfers

Section 16 governs cross-border transfers of personal data. The provision adopts a permissive approach:

1. The Central Government may, after assessment of relevant factors, notify countries or territories outside India to which personal data **shall not be transferred**.
2. In the absence of such notification, personal data may be transferred to any country or territory outside India, subject to the terms and conditions prescribed by the Central Government.

This approach differs from the adequacy-based system of the GDPR, where transfers are permitted only to countries deemed to provide adequate protection or where appropriate safeguards are in place. The DPDP Act's restrictive list approach provides greater flexibility for data transfers but has raised concerns regarding the adequacy of protection in recipient jurisdictions.

5.9 Exemptions

Section 17 empowers the Central Government to exempt government agencies from provisions of the Act in the interests of:

- Sovereignty and integrity of India
- Security of the State
- Friendly relations with foreign States
- Maintenance of public order
- Prevention, detection, investigation, or prosecution of offences

The breadth of these exemptions has attracted criticism for potentially undermining the data

[29] Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s.9.

ISSN: 2582-6433

protection rights of individuals vis-à-vis the State[30].

Section 17(2) additionally exempts:

- Processing necessary for research, archival, or statistical purposes
- Processing by start-ups or other classes of data fiduciaries as notified by the Central Government
- Processing necessary for enforcing any legal right or claim

5.10 Data Protection Board of India

Chapter V establishes the Data Protection Board of India (DPBI) as the adjudicatory and enforcement authority under the Act.

5.10.1 Composition

Section 19 provides for the establishment of the DPBI. The Board shall consist of a Chairperson and such other Members as the Central Government may appoint. The Chairperson and Members shall be persons of ability, integrity, and standing, having special knowledge or experience in the fields of data governance, data protection, information technology, data management, data analytics, law, administration, or public administration.

5.10.2 Powers and Functions

Section 27 empowers the Board to:

1. Determine non-compliance with the provisions of the Act
2. Direct data fiduciaries to take necessary measures
3. Impose penalties for non-compliance
4. Accept voluntary undertakings from data fiduciaries
5. Examine data breaches and issue appropriate directions

The Board shall function as a digital office and proceedings shall ordinarily be conducted through digital means.

5.10.3 Penalties

Section 33 and the Schedule to the Act prescribe penalties for various contraventions[31]:

Contravention	Penalty
Failure to take reasonable security safeguards to prevent personal data breach	Up to ₹250 crore
Failure to notify the Board and affected data principals of personal data breach	Up to ₹200 crore

[30] Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s.17.
[31] Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s.33.

ISSN: 2582-6433

Non-fulfillment of additional obligations relating to children	Up to ₹200 crore
Non-fulfillment of additional obligations of Significant Data Fiduciaries	Up to ₹150 crore
Breach of any other provision of the Act or rules	Up to ₹50 crore

Section 33(2) provides that in determining the quantum of penalty, the Board shall have regard to:

- Nature, gravity, and duration of the breach
- Type of personal data affected
- Repetitive nature of the breach
- Whether the data fiduciary realized any financial gain or avoided any financial loss due to the breach
- Actions taken by the data fiduciary to mitigate effects of the breach
- Whether the penalty to be imposed is proportionate and effective.

7. Judicial Developments in Data Privacy

7.1 Pre-Puttaswamy Jurisprudence

Prior to the definitive recognition of the right to privacy in *Puttaswamy*, Indian courts grappled with data protection issues in various contexts.

In *PUCL v. Union of India*, the Supreme Court considered the constitutionality of telephone tapping. The Court recognized that telephone tapping constitutes an invasion of privacy and established guidelines for lawful interception, requiring authorization by the Home Secretary at the appropriate level, recording of reasons, and review mechanisms[32].

The case of *R. Rajagopal v. State of T.N.* established the contours of the right to privacy in the context of publications. The Court recognized that individuals have a right to be let alone, and unauthorized publication of private information could be actionable. However, the Court also held that once matters become part of public records, the right to privacy yields to the right to information.

In *District Registrar and Collector, Hyderabad v. Canara Bank*, the Supreme Court observed that the right to privacy deals with persons and not places, and that individuals have a legitimate expectation of privacy regarding their personal records and information.

[32] *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301: AIR 1997 SC 568.

ISSN: 2582-6433

7.2 Data Protection in Employment Context

Several High Court decisions have addressed data protection issues in employment relationships.

In *Bharat Sanchar Nigam Limited v. Telephone Regulatory Authority of India*, the Delhi High Court considered whether call data records of employees could be disclosed. The Court observed that employees have a reasonable expectation of privacy in their personal communications, even when using employer-provided devices.

The question of workplace surveillance and employee privacy has been considered in various industrial disputes, with tribunals and courts attempting to balance employer interests in monitoring with employee privacy rights.

7.3 Judicial Treatment of Data Breaches

Indian courts have increasingly been called upon to address data breach incidents and their consequences.

In *Jayesh Thakor v. Union of India*, a PIL challenging the data breach at CoWIN (the Covid-19 vaccination platform), the Supreme Court directed the Centre to conduct a probe into the alleged data breach and submit a report. The Court emphasized the importance of data security in government platforms handling sensitive health information.

High Courts have also entertained petitions seeking action against data breaches by private entities. In *Nandini Delany v. Instagram*, the Karnataka High Court directed Instagram to block profiles impersonating the petitioner and using her personal data without consent, recognizing the harm caused by unauthorized use of personal information on social media platforms.

7.4 Social Media and Privacy

The relationship between social media platforms and user privacy has generated significant litigation.

In *Shreya Singhal v. Union of India*, while primarily addressing the constitutionality of Section 66A of the IT Act, the Supreme Court also considered the liability of intermediaries under Section 79. The Court's interpretation of the "actual knowledge" standard has implications for data protection, as it defines when intermediaries become liable for hosting user-generated content that may violate privacy.

The WhatsApp Privacy Policy case, *Karmanya Singh Sareen v. Union of India*, addressed concerns about WhatsApp's updated privacy policy that expanded data sharing with its parent company, Meta. The Delhi High Court directed WhatsApp to delete data collected from users

ISSN: 2582-6433

who had not opted into the new policy by September 25, 2016, and to comply with requirements under the IT Act and SPDI Rules[33].

7.5 Aadhaar Litigation

The Aadhaar scheme has been the subject of extensive litigation, reflecting the tensions between digital governance and privacy.

Beyond the main *Puttaswamy* (Aadhaar) judgment, numerous cases have addressed specific aspects of Aadhaar linkage. In *Binoy Viswam v. Union of India*, the Supreme Court examined the mandatory linkage of Aadhaar with Permanent Account Numbers under Section 139AA of the Income Tax Act, 1961, and upheld the requirement, finding it did not violate the right to privacy as it served the legitimate aim of preventing tax evasion.

7.6 Pegasus Spyware Case

One of the most recent and significant privacy-related matters is the Pegasus spyware controversy. Although not a final judgment on merits, the Supreme Court in *Manohar Lal Sharma v. Union of India* (2021)[34] constituted a technical committee to investigate allegations of unauthorized surveillance using Pegasus spyware.

The Court observed that:

- The right to privacy cannot be compromised without due process
- Surveillance allegations require judicial scrutiny
- National security cannot be used as a blanket justification to deny transparency

This case reflects the judiciary's growing concern over digital surveillance and cyber intrusion.

7.7 Recent Developments

Post-DPDP Act judicial developments continue to shape data privacy jurisprudence.

Courts have begun referencing the DPDP Act in their decisions, signaling its integration into the broader legal framework. In various writ petitions challenging surveillance activities and data collection by state agencies, petitioners have invoked the DPDP Act alongside constitutional provisions.

The implementation of the DPDP Act will likely generate substantial litigation as its provisions are tested in specific factual contexts, and the jurisprudence of the Data Protection Board

[33] *Karmanya Singh Sareen v. Union of India*, W.P. (C) No. 7663 of 2016, Delhi High Court, order dated 23 September 2016.
[34] Manohar Lal Sharma v. Union of India, W.P. (C) No. 993/2021 (Supreme Court of India).

ISSN: 2582-6433

evolves.

8.Comparative Analysis

8.1 European Union: General Data Protection Regulation

8.1.1 Introduction

A comparative analysis of data protection laws helps in understanding the strengths and weaknesses of the Indian legal framework in relation to global standards. In the digital age, data flows transcend national boundaries, making it essential for domestic laws to align with international best practices.

One of the most advanced and widely referenced data protection frameworks globally is the General Data Protection Regulation (GDPR), which has set high standards for privacy protection and influenced many jurisdictions, including India

8.1.2 Scope and Applicability

One of the most significant similarities between the GDPR and the DPDP Act is their broad territorial scope.

The GDPR applies to organizations established within the European Union as well as entities outside the EU that process personal data of EU residents for offering goods or services or monitoring their behavior. It covers both automated and non-automated processing of personal data contained in filing systems.

The DPDP Act applies to digital personal data processed within India and also extends to entities outside India if they offer goods or services to individuals in India. However, unlike the GDPR, the Indian law focuses only on digital personal data and excludes offline personal data unless digitized.

Another distinction lies in the treatment of non-personal data[35]. The GDPR exclusively governs personal data, whereas earlier Indian proposals attempted to regulate non-personal data as well. The final DPDP Act, however, restricts itself to personal data.

8.1.3 Comparison between India and GDPR

Basis	India	GDPR
Nature of Rights	Limited individual rights	Extensive rights (erasure, portability)
Enforcement	Developing authority	Strong independent regulators
Penalties	Moderate	Very high (up to 4% global turnover)
Cross-border data	Government controlled	Strict transfer rules

[35] Digital Personal Data Protection Act, 2023; General Data Protection Regulation (EU) 2016/679.

ISSN: 2582-6433

The GDPR, which came into effect in 2018, is often considered the gold standard of data protection legislation. Compared to the GDPR, the DPDP Act[36]:

- Does not include the right to data portability
- Has a narrower set of lawful bases for processing
- Provides for substantially lower maximum penalties
- Does not include explicit provisions for Data Protection Impact Assessments for all high-risk processing
- Adopts a restrictive list approach to cross-border transfers rather than adequacy assessments

However, the DPDP Act's simpler structure and focus on digital personal data may make compliance more manageable in the Indian context.

8.2 United States

Unlike the EU and India, the United States lacks comprehensive federal data protection legislation, relying instead on sector-specific laws such as the Health Insurance Portability and Accountability Act (HIPAA) for health data and the Gramm-Leach-Bliley Act for financial data. State-level legislation, particularly the California Consumer Privacy Act and California Privacy Rights Act, have emerged as significant regulatory frameworks.

India's approach of comprehensive legislation applicable across sectors provides greater coherence than the fragmented US approach, though sector-specific rules continue to supplement the general framework.

8.3 China: Personal Information Protection Law

China's Personal Information Protection Law, 2021 (PIPL), provides a useful comparator as a data protection framework in a developing economy. Like the DPDP Act, PIPL emphasizes state interests and contains significant government exemptions. However, PIPL includes data portability rights and stricter cross-border transfer provisions requiring security assessments for certain transfers.

9. Challenges and Emerging Issues

9.1 Challenges

The effective implementation of the DPDP Act faces several challenges:

[36] Digital Personal Data Protection Act, 2023; General Data Protection Regulation (EU) 2016/679.

ISSN: 2582-6433

9.1.1 Institutional Capacity

The Data Protection Board of India is tasked with substantial responsibilities including complaint adjudication, breach notification processing, and enforcement. Building adequate institutional capacity, technical expertise, and procedural infrastructure presents a significant challenge, particularly given the volume of data processing occurring in India's digital economy.

9.1.2 Consent Fatigue and Meaningful Consent

The consent-based framework, while conceptually sound, faces practical challenges in implementation. "Consent fatigue," where individuals routinely click through consent notices without comprehension, undermines the effectiveness of consent as a protective mechanism. Ensuring that consent is truly informed and meaningful, rather than a mere formality, requires innovation in consent mechanisms and user interfaces.

9.1.3 Enforcement Against Foreign Entities

The extraterritorial application of the DPDP Act to entities processing data of individuals in India raises enforcement challenges. Establishing jurisdiction, serving notices, and enforcing orders against foreign entities with no physical presence in India presents practical difficulties.

9.1.4 Awareness and Compliance

For micro, small, and medium enterprises that process personal data, understanding and complying with data protection requirements may be challenging due to limited resources and technical expertise. Building awareness and facilitating compliance across the spectrum of data fiduciaries is essential for the Act's effectiveness.

9.2 Gaps in the Legal Framework

Several gaps and concerns have been identified in the DPDP Act:

9.2.1 Government Exemptions

The broad exemptions for government agencies in Section 17 have attracted criticism for potentially undermining data protection vis-à-vis the State. The lack of independent oversight over government data processing raises concerns about accountability.

9.2.2 Absence of Data Protection Authority Independence

Unlike regulatory models in other jurisdictions where data protection authorities enjoy substantial independence, the DPDP Act provides for significant government control over the Data Protection Board, including appointments and terms of service. This raises questions about the Board's independence and ability to hold government entities accountable.

ISSN: 2582-6433

9.2.3 Limited Rights

Compared to frameworks like the GDPR, the DPDP Act provides a narrower set of data principal rights. Notably, the Act does not include:

- A right to data portability
- A right not to be subject to automated decision-making
- Explicit provisions for compensation for data principals

9.2.4 Journalistic and Civil Society Exemptions

The DPDP Act does not contain specific exemptions for journalistic activities or civil society organizations processing personal data for public interest purposes, which could have implications for freedom of the press and civic space.

9.3 Emerging Issues

Several emerging issues require attention as India's data protection framework evolves:

9.3.1 Artificial Intelligence and Automated Decision-Making

The rapid deployment of artificial intelligence systems raises questions about algorithmic accountability, automated decision-making affecting individuals, and the use of personal data for AI training. The DPDP Act does not contain specific provisions addressing AI, creating a potential regulatory gap.

9.3.2 Surveillance and National Security

Balancing data protection with national security imperatives remains contentious. The breadth of government exemptions and surveillance powers under laws such as the Telegraph Act, 1885, and IT Act, 2000, raise ongoing concerns about proportionality and oversight.

9.3.3 Children's Data and Age Verification

Implementing the Act's provisions on children's data, including verifiable parental consent and prohibitions on tracking and targeted advertising, presents technical and practical challenges around age verification without creating additional privacy intrusions.

10 Conclusion and Recommendations

10.1 Summary of Findings

This paper has undertaken a comprehensive analysis of the legal framework governing data privacy in India. The key findings may be summarized as follows:

Constitutional Foundation: The right to privacy has been conclusively established as a fundamental right under Article 21 of the Constitution through the *Puttaswamy* judgment. The right encompasses informational privacy, providing constitutional grounding for data

ISSN: 2582-6433

protection legislation. The proportionality standard articulated in *Puttaswamy* serves as the benchmark for evaluating the constitutionality of laws impacting privacy.

Pre-DPDP Act Framework: The Information Technology Act, 2000, and the SPDI Rules, 2011, provided the primary statutory framework for data protection prior to 2023. While these instruments introduced important concepts such as consent, purpose limitation, and security requirements, they suffered from limitations including narrow applicability, inadequate enforcement mechanisms, and absence of an independent supervisory authority.

Digital Personal Data Protection Act, 2023: The DPDP Act represents a significant milestone in India's data protection journey. It establishes a comprehensive framework with defined rights for data principals, obligations for data fiduciaries, special protections for children, and an enforcement mechanism through the Data Protection Board. However, concerns remain regarding government exemptions, regulatory independence, and the scope of data principal rights.

Sector-Specific Regulations: Data protection in India involves a complex interplay between the general framework and sector-specific regulations in banking, telecommunications, healthcare, and the Aadhaar ecosystem. These sectoral rules address unique risks and requirements of their respective domains but must be harmonized with the DPDP Act.

Judicial Contributions: Courts have played a crucial role in developing data privacy jurisprudence, from the foundational *Puttaswamy* decisions to specific rulings on data breaches, social media privacy, and Aadhaar linkage. Continued judicial engagement will be essential in interpreting and applying the DPDP Act.

10.2 Recommendations

Based on the analysis undertaken, the following recommendations are offered for strengthening India's data privacy framework:

10.2.1 Enhance Regulatory Independence

The Data Protection Board should be constituted with greater independence from the executive to ensure effective and impartial enforcement, including against government entities. This could include fixed terms for members, transparent appointment processes involving judicial or legislative oversight, and protection against arbitrary removal.

10.2.2 Strengthen Accountability for Government Processing

The exemptions for government agencies should be narrowed and made subject to independent oversight. Processing of personal data by government entities should require periodic audits, impact assessments, and reporting to Parliament or an independent body. Surveillance activities

ISSN: 2582-6433

should be brought under a comprehensive framework with judicial authorization requirements.

10.2.3 Expand Data Principal Rights

Consideration should be given to incorporating additional rights such as:

- Right to data portability to promote competition and individual control
- Right not to be subject to decisions based solely on automated processing
- Explicit right to compensation for violations
- Right to explanation for automated decisions affecting individuals

10.2.4 Address AI and Emerging Technologies

The regulatory framework should be updated to address specific risks posed by artificial intelligence, including requirements for algorithmic transparency, human oversight of automated decisions, and restrictions on certain high-risk AI applications involving personal data.

10.2.5 Facilitate Compliance for MSMEs

Given the significant compliance burden that comprehensive data protection legislation may impose on small enterprises, dedicated guidance, simplified compliance pathways, and capacity-building measures should be developed to facilitate compliance by micro, small, and medium enterprises.

10.2.6 Strengthen Cross-Border Transfer Provisions

While the restrictive list approach provides flexibility, clearer criteria for notification of restricted countries and mechanisms for assessing protection adequacy in recipient jurisdictions would enhance certainty and alignment with international standards.

10.2.7 Civil Society and Journalistic Protections

Appropriate exemptions or modified requirements for journalistic activities and civil society organizations processing data in the public interest should be considered to protect freedom of expression and civic space.

10.2.8 Promote Privacy-by-Design

Beyond technical compliance, a culture of privacy protection should be fostered through requirements for privacy-by-design and privacy-by-default in the development of systems and products that process personal data.

10.3 Concluding Observations

The legal framework governing data privacy in India has evolved substantially over the past two decades, from fragmented provisions to a comprehensive statutory regime. The recognition

ISSN: 2582-6433

of privacy as a fundamental right in *Puttaswamy*[37] and the enactment of the Digital Personal Data Protection Act, 2023, represent landmark developments that position India alongside other jurisdictions with dedicated data protection laws.

However, the mere existence of legislation is insufficient to guarantee effective protection of data privacy. The true test will lie in implementation: the constitution and functioning of the Data Protection Board, the interpretation of statutory provisions through enforcement actions and judicial decisions, the development of subordinate legislation that gives effect to the Act's principles, and the building of a culture of privacy consciousness among organizations and individuals.

As India's digital economy continues to expand, bringing billions of data points into the ambit of processing, the stakes of getting data protection right become ever higher. The framework must balance multiple objectives: protecting individual rights and dignity, enabling beneficial data use for innovation and public services, ensuring security and preventing harm, and maintaining competitiveness in the global digital economy.

The journey towards comprehensive data protection in India is far from complete. Continued legislative refinement, regulatory development, judicial interpretation, and public engagement will be necessary to build a framework that truly serves the goal articulated in the *Puttaswamy* judgment: a free and fair digital economy that protects privacy and empowers Indians.

11. Bibliography

Statutes and Legislations

1. Constitution of India, 1950.
2. Information Technology Act, 2000 (Act 21 of 2000).
3. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
5. Digital Personal Data Protection Act, 2023 (Act 22 of 2023).
6. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
7. Clinical Establishments (Registration and Regulation) Act, 2010.
8. General Data Protection Regulation (EU) 2016/679.

[37] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

ISSN: 2582-6433

Key Cases

1. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
2. *K.S. Puttaswamy (Aadhaar) v. Union of India*, (2019) 1 SCC 1.
3. *M.P. Sharma v. Satish Chandra*, AIR 1954 SC 300.
4. *Kharak Singh v. State of Uttar Pradesh*, AIR 1963 SC 1295.
5. *Gobind v. State of Madhya Pradesh*, (1975) 2 SCC 148.
6. *People's Union for Civil Liberties (PUCL) v. Union of India*, (1997) 1 SCC 301.
7. *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.
8. *District Registrar and Collector v. Canara Bank*, (2005) 1 SCC 496.
9. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
10. *Binoy Viswam v. Union of India*, (2017) 7 SCC 59.
11. *WhatsApp LLC v. Reserve Bank of India*, Writ Petition (Civil) No. 1041 of 2018, Supreme Court of India.
12. *Karmanya Singh Sareen v. Union of India*, W.P. (C) No. 7663 of 2016, Delhi High Court.
13. *Manohar Lal Sharma v. Union of India*, W.P. (C) No. 993/2021, Supreme Court of India.

Reports, Guidelines and Government Publications

1. Ministry of Electronics and Information Technology, Government of India, *Report of the Committee of Experts on Data Protection (Srikrishna Committee Report)*, 2018.
2. Ministry of Health and Family Welfare, Government of India, *National Digital Health Mission: Health Data Management Policy*, 2020.
3. Telecom Regulatory Authority of India, *Recommendations on Privacy, Security and Ownership of Data in the Telecom Sector*, New Delhi, 16 July 2018.
4. Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, 2021.
5. Reserve Bank of India, *Master Direction on Non-Banking Financial Company – Account Aggregator*, 2016.
6. Ministry of Communications and Information Technology, Government of India, G.S.R. 313(E), dated 11 April 2011.