DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CONSTITUTIONAL AND COMPARATIVE ANALYSIS

Altamash Farahat, Vishwakarma University, Pune

1. Introduction

Digital transformation has changed how people interact with both markets and government entities. The modern digital economy treats personal data as both a valuable economic resource and a tool for administrative efficiency while exposing citizens to various constitutional rights violations. India has become a global leader in internet usage while experiencing rapid expansion of its digital payment systems and biometric identification networks and e-governance platforms and fintech ecosystems and artificial intelligence solutions. The rapid growth of data-dependent technologies has increased public apprehension about three main areas which include surveillance activities and their associated profiling techniques and the wrongful use of confidential information.

People now consider privacy protection as a basic constitutional right because personal data has become vital for contemporary society. The current digital environment allows continuous collection and storage of personal data which used to be limited to direct information exchanges during earlier time periods. Data breaches together with unauthorized disclosures have resulted in identity theft and reputational harm and financial exploitation of individuals. The creation of state-operated data collection systems results in major difficulties because they enable surveillance operations while lacking proper democratic oversight mechanisms.

India did not establish complete legal regulations for personal data protection until multiple years passed. The main regulatory protections of the country derived from the Information Technology Act of 2000 and its accompanying regulations which included Section 43A and the Sensitive Personal Data or Information Rules of 2011. The legal provisions implemented between these two points contained two main limitations because they focused on certain outcomes and failed to establish complete legal rights for people and create a regulatory body with complete enforcement authority. The legal provisions implemented between these two points contained two main limitations because they focused on certain outcomes and failed to establish complete legal rights for people and create a regulatory body with complete

enforcement authority.

The Supreme Court of India established a new constitutional framework through its 2017 decision which the nine-judge bench reached in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India when it declared that the right to privacy exists as an essential part of Article 21 of the Constitution. The Court recognized privacy as encompassing informational self-determination, decisional autonomy, and bodily integrity. The judgment established the proportionality doctrine as the main standard which governs assessments of state actions that limit people's right to privacy. The legal framework requires all privacy restrictions to fulfill three essential conditions about their validity and purpose and their execution and actual impacts.

The Puttaswamy decision required the legislature to create a complete data protection law framework for implementation. The Government formed the Justice B.N. Srikrishna Committee which recommended the development of a rights-oriented Personal Data Protection Bill during 2018. The Digital Personal Data Protection Act 2023 represents the final outcome of multiple legislative revisions which led to its official passage.

The DPDP Act serves as India first complete law which specifically regulates digital personal data. The law establishes a consent-based data processing system which requires data fiduciaries to fulfill their responsibilities while data principals receive enforceable rights and the Data Protection Board of India functions as the adjudicative body. The Act establishes substantial financial penalties for organizations that fail to comply with its regulations while it uses a notification system for organizations that need to transfer data across international borders.

Nonetheless, the enactment of a statute does not alone translate into effective protection of constitutional rights. This raises the question of structure. Is it truly going to operationalize the proportionality standards articulated in Puttaswamy? Does it risk undermining privacy safeguards by providing a broad governmental exemption? Does the Data Protection Board’s organizational structure ensure its regulatory independence? How does India's legislation compare to data protection regimes in the international domain, notably the European Union's General Data Protection Regulation (GDPR)?

This article provides for a comprehensive constitutional and comparative analysis of the DPDP

Act, 2023, contending that while the Act portends a significant normative improvement in India's cyberspace governance apparatus; its actual efficacy will ride upon judicial interpretation, institutional independence, and principled rule-making. The sub-division structure in the enactment makes it somewhat flexible from an administrative aspect, yet some are scrutinized for concerns concerning structural safeguards, particularly focusing on executive exemptions and parliamentary control structure.

In summary, the article aims to assess whether India has successfully transitioned from constitutional recognition of privacy to meaningful statutory enforcement of informational autonomy, through the prism of positioning it within the broader evolution of privacy law in India and global data protection developments.

2. Constitutional Foundations of Privacy in India

The constitutional recognition of privacy rights in India developed through a non-linear process that lasted for multiple years until it reached its final form in 2017. The Digital Personal Data Protection Act of 2023 requires evaluation through its judicial development which establishes its constitutional requirements and normative power.

2.1 Early Judicial Ambivalence

The Indian Constitution does not explicitly grant citizens a fundamental right to privacy. The initial constitutional court cases faced confusion regarding their decision to recognize privacy as a fundamental right. The Supreme Court used the Kharak Singh v. State of Uttar Pradesh case to evaluate whether police surveillance legislation met constitutional standards. The court ruling established that domiciliary visits violated constitutional rights while the court established that general privacy rights do not exist. Justice Subba Rao's dissenting opinion created vital judicial standards by establishing that surveillance techniques violated personal liberties protected under Article 21.

Subsequently, in Govind v. State of Madhya Pradesh, the Court moved closer to acknowledging privacy as a constitutional interest. While not declaring it an absolute right, the Court recognized that privacy could be derived from Articles 19 and 21 and may be subject to reasonable restrictions. The decision introduced the idea that privacy interests must be balanced against compelling state interests, thereby foreshadowing later proportionality analysis.

In People's Union for Civil Liberties (PUCL) v. Union of India, the Court examined the legality of telephone tapping under the Telegraph Act. It recognized that unauthorized interception of communications constitutes a serious invasion of privacy and prescribed procedural safeguards to regulate surveillance. This judgment reinforced the understanding that informational privacy falls within constitutional protection, even though it remained doctrinally unsettled.

The early decisions show that judicial bodies started to recognize privacy rights as an essential component of personal freedom even though privacy rights had not yet been formally established in law. The 2017 landmark judgment remained the first time that a clear constitutional definition of constitutional rights existed.

2.2 The Transformative Judgment: Justice K.S. Puttaswamy

The nine-judge bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India established a landmark judgment which transformed Indian constitutional law. The Court unanimously affirmed that privacy is a fundamental right protected under Part III of the Constitution. The judgment overruled earlier precedents that had denied or diluted privacy protection and established a strong theoretical basis which depended on dignity and autonomy and individual freedom rights.

The Court defined privacy as a multi-dimensional right which includes:

- Bodily privacy, protecting physical integrity;
- Decisional autonomy, safeguarding personal choices;
- Informational privacy, governing control over personal data.

The constitutional recognition of informational privacy as a fundamental right represents a crucial development for data protection legislation. The Court recognized that nowadays people require control over their personal data because this ability constitutes an essential part of their dignity rights.

The judgment established proportionality as the main standard which judges privacy restriction assessment. The entire system requires all four elements to be present before it can operate:

1. Legality – The restriction must have a basis in law.
2. Legitimate Aim – The objective must serve a legitimate state purpose.
3. Necessity – The measure must be necessary and the least restrictive alternative.
4. Balancing (Proportionality Stricto Sensu) – The extent of interference must not outweigh the intended benefits.

The doctrinal framework establishes essential legal restrictions which both legislative bodies and executive agencies must follow. All data protection laws require interpretation through the framework of proportionality rules.

2.3 Informational Self-Determination

The Puttaswamy ruling recognizes informational privacy which demonstrates a global understanding of informational self-determination that the German Federal Constitutional Court first defined. The principle establishes that individuals must maintain authority over all stages of their personal data which includes its collection processing and distribution.

In India informational self-determination requires that consent mechanisms must provide actual understanding to users instead of creating deceptive options. Privacy policies and click-through agreements do not automatically fulfill constitutional requirements because people need authentic selection power and complete comprehension of the documents.

The DPDP Act requires consent-based processing because it serves as a legal attempt to implement informational self-determination. The constitution mandates that all consent requirements must remain free to users who need to provide complete information about their choice which they should be able to withdraw at any time without facing serious repercussions.

2.4 Privacy as a Horizontal Right

The Puttaswamy judgment establishes privacy rights as existing between citizens and all entities, not just governmental bodies. The Court recognized that digital age privacy threats exist because non-government entities can violate fundamental rights, which people can enforce against state authorities. The observation creates major effects for data protection law because private companies control substantial amounts of personal data, which they process in

their operations.

The DPDP Act therefore serves not only as a regulatory statute but also as an instrument of constitutional horizontal effect. The law establishes rules for private data fiduciaries because the State must fulfill its duty to safeguard basic human rights.

2.5 Constitutional Implications for the DPDP Act

The constitutional recognition of privacy rights establishes data protection requirements as essential constitutional obligations instead of optional policy choices. The DPDP Act requires all its provisions to pass testing that uses proportionality standards as evaluation criteria. The assessment of broad exemptions together with executive discretion and enforcement structures needs to follow the constitutional requirement which demands a balance between state interests and individual rights.

The DPDP Act establishes its legitimacy through two factors which combine parliamentary approval with its conformity to constitutional legal standards. The provisions of this statute allow for excessive government monitoring which will lead to judicial review because it enables excessive government monitoring. The Act will help improve India's digital constitutionalism when it is applied according to its constitutional protections.

3. Legislative Evolution of Data Protection in India

The Digital Personal Data Protection Act 2023 received its first official enactment through India and its historical development process which began more than 20 years ago. The Digital Personal Data Protection Act requires people to access its main rules through its entire document. The Digital Personal Data Protection Act requires people to access its main rules through its entire document according to its normative and structural elements.

3.1 The Information Technology Act, 2000: A Limited Beginning

India's first official law for data protection was established through the Information Technology Act of 2000. The law which enables electronic commerce and recognizes digital signatures was established without a complete design for privacy protection. The law now includes provisions for data protection which were added through subsequent amendments.

The Act's Section 43A established a standard which required businesses to protect sensitive personal information through proper security protocols. Negligent behavior that resulted in wrongfully lost or gained assets could lead to compensation at court. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011 established different types of sensitive personal data which include passwords and financial data and medical records and biometric information.

The IT Act framework failed to establish effective digital security protection through its existing rules. The law mainly targeted corporate entities while it failed to create suitable rules for government organizations which handle data processing. The system did not include a rights-based framework which would have let people control their personal information. The system lacked effective enforcement methods which focused on compensating victims instead of enforcing rules. The digital ecosystems which developed during the 2010s showed increasing evidence of the system's incomplete design because it used multiple separate security systems.

3.2 Constitutional Mandate and the Srikrishna Committee

The recognition of privacy as a fundamental right in 2017 created an explicit constitutional obligation for legislative reform. The Government of India established a Committee of Experts which Justice B.N. Srikrishna chaired to create a complete data protection legislation. The Committee's 2018 report A Free and Fair Digital Economy Protecting Privacy Empowering Indians established the basic principles which Indian data protection laws use today.

The Srikrishna Committee proposed a robust, rights-based framework which took inspiration from the European Union's GDPR. The organization needed to create a Data Protection Authority which would operate independently, while the document established rules for processing data and specified which types of personal information needed to be stored in locations. The report established accountability, transparency and enforcement as the main elements of the proposed system.

The Committee established its main purpose as twofold because it needed to protect privacy and drive digital progress. The organization established data protection as a system which helps build trust because organizations need it to develop their digital operations sustainably.

3.3 The Personal Data Protection Bill, 2019

The Personal Data Protection Bill 2019 was presented to Parliament because the Committee recommended its introduction. The Bill included multiple proposals from the Committee which it incorporated into its text:

- A comprehensive definition of personal and sensitive personal data;
- Explicit rights such as data portability and the right to be forgotten;
- Mandatory data localization requirements;
- Establishment of a Data Protection Authority with regulatory independence;
- Structured obligations for data fiduciaries and significant data fiduciaries.

The Bill created a prolonged discussion which lasted for an extended period. Industry stakeholders raised concerns about two specific issues which included compliance burdens and localization requirements. Civil society groups expressed apprehension about broad governmental exemption powers that could potentially undermine privacy safeguards.

The Joint Parliamentary Committee received the Bill as a referral after which it recommended various changes. The Government decided to withdraw the 2019 Bill after extended discussions which took place until 2022. This decision marked a transition to a more efficient and straightforward system.

3.4 Transition to the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act of 2023 establishes its own rules which differ from the previous draft that contained extensive regulatory details. The final statute adopts a more concise drafting style and introduces notable structural changes.

The Act restricts its application to digital personal data while it does not cover non-digital records until those records become digital. The system now permits international data movement through approved countries after organizations notify authorities about their information transfer activities. The proposed independent Data Protection Authority will be replaced by a Data Protection Board whose members will be appointed by the Central

Government with set conditions for their appointment and service.

The new rules provide authorities with the ability to regulate businesses while still permitting companies to operate their activities. The Act requires organizations to obtain user consent for data processing activities while maintaining their legal compliance requirements through simplified regulations. Critics of the new regulation state that its efforts to simplify operations will result in decreased power for organizations which protect civil rights and thus jeopardize their ability to carry out their mission.

3.5 Legislative Philosophy and Policy Orientation

The legislative evolution from the IT Act to the DPDP Act demonstrates a gradual movement from sectoral and reactive regulation toward a consolidated privacy framework. The research demonstrates that policy orientation exists because economic pragmatism shapes governmental decisions.

The DPDP Act appears to adopt a growth-compatible regulatory philosophy. The legislative body establishes digital entrepreneurship and foreign investment through its decision to eliminate strict localization rules and its plan to decrease mandatory compliance requirements. The company establishes its commitment to accountability through its implementation of major penalties which will be applied to any instances of non-compliance.

The DPDP Act establishes its unique approach through two main strategies which combine privacy protection with the creation of an environment that supports innovation. The success of this balance will depend on how interpretation standards and enforcement operations develop.

3.6 From Fragmentation to Framework

The country now has its first dedicated data protection law which follows both constitutional court rulings and international security regulations. The development of better laws does not ensure that organizations will achieve effective protective measures. The evaluation of the framework's actual strength requires complete structural assessment.

The following section therefore examines the architecture of the DPDP Act, 2023, assessing its consent mechanisms, rights structure, regulatory design, and enforcement.

4. Structural Analysis of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 establishes India's first complete legal system which controls digital personal data. The DPDP Act creates a complete framework which defines different roles and processing methods and enforcement systems and penalty methods in contrast to previous disjointed rules under the Information Technology Act. The framework requires thorough examination because it contains both advantages and disadvantages.

4.1 Scope and Applicability

The Act applies to digital personal data processed within India, as well as to processing conducted outside India if it relates to offering goods or services to individuals within India. This extraterritorial reach connects the Indian system to international standards which especially include the European Union's General Data Protection Regulation (GDPR).

The Act restricts its scope to digital personal data while excluding non-digital records which require digitization to become applicable. The current enforcement practice allows law enforcement officials to take their required steps but it creates security vulnerabilities because physical records remain unprotected until they enter digital storage.

The statute extends its coverage to all processing activities conducted by government and private sector entities regardless of their operations. This represents a substantial change from the previous IT Act framework which centered its attention on corporate entities.

4.2 Key Definitions and Conceptual Framework

The DPDP Act Design features a triple framework, constituted of several Legislative Components:

1. Data Principal – The individual to whom the personal data relates.
2. Data Fiduciary – The entity that determines the purpose and means of processing personal data.
3. Data Processor – An entity that processes data on behalf of a Data Fiduciary.

The term "fiduciary" holds special significance because it serves as a central element in legal

practice. Fiduciary relationships in traditional legal doctrine create obligations that require parties to maintain trust, loyalty, and good faith toward each other. The Act establishes a standard for fiduciary duties but it stops short of defining these duties as strict equitable obligations because the terminology used establishes a standard for proper management duties.

Any data that identifies an individual to whom it relates constitutes personal data according to its broad definition. This definition is intentionally broad because it needs to encompass various digital identifiers that exist today.

4.3 Consent Architecture

Consent lies at the heart of the DPDP framework. The Act mandates that consent must be:

- Free
- Specific
- Informed
- Unambiguous
- Given through clear affirmative action

Your consent needs to include a notification which describes the processing purpose and the data collection methods and the rights that individuals can use to access their information.

The Act requires that users should be able to withdraw their consent with the same difficulty which they had when they gave their permission. The system prevents organizations from using "consent lock-in" practices which take away user control.

The situation presents two obstacles that must be addressed. The digital ecosystems designed with their extensive privacy policies and complex technical disclosures only enable users to provide procedural consent which does not meet their actual consent needs. People need to understand information at a deep level to achieve real informational autonomy which requires more than basic consent.

4.4 Legitimate Uses and Non-Consent Processing

The Act allows processing without consent for specific legitimate uses. The approved uses

include state functions and legal obligation compliance and medical emergency response and employment-related activities.

The inclusion of legitimate use provisions reflects practical governance needs. The interpretation of these clauses must be restricted because their excessive scope will diminish consent-based protection measures. The provisions will weaken the Act's focus on personal autonomy if they receive broad application.

The main challenge exists because authorities must maintain narrow and appropriate limits on legitimate use exceptions to achieve their intended goals.

4.5 Rights of Data Principals

The DPDP Act grants individuals several enforceable rights, including:

- The right to obtain information regarding processing of their personal data.
- The right to correction and erasure of inaccurate or outdated data.
- The right to grievance redressal.
- The right to nominate another person to exercise rights in case of death or incapacity.

The IT Act framework which did not provide any defined rights for individuals now becomes transformed by these rights which establish new rights for individuals. The Act does not grant a data portability right or a complete right to be forgotten which the GDPR offers.

The absence of certain advanced rights may reflect a deliberate policy choice to simplify compliance. The existing rules for digital market portability rights remain insufficient because they do not enable users to manage their online activities.

4.6 Obligations of Data Fiduciaries

Data Fiduciaries are subject to several obligations, including:

- Implementing reasonable security safeguards to prevent data breaches.
- Notifying the Data Protection Board and affected individuals in the event of a breach.

- Ensuring accuracy of data where necessary.
- Deleting personal data upon completion of purpose.

The Act requires organizations to establish operational security measures which will create a compliance-based work environment because it prohibits organizations from facing legal penalties until after an actual harmful event has taken place.

The authorities will identify particular organizations as Significant Data Fiduciaries according to their data handling capabilities and the potential threats they present to individual privacy rights. The organizations must fulfill additional legal requirements which include designating Data Protection Officers and conducting regular assessment processes.

The tiered regulatory framework demonstrates risk-based governance principles which international data protection systems use as their standard method of operation.

4.7 Data Protection Board of India

The Act establishes the Data Protection Board of India as the adjudicatory authority responsible for enforcement. The Board is empowered to:

- Conduct inquiries into non-compliance.
- Impose monetary penalties.
- Direct remedial measures.

The Central Government establishes both the Board's composition and its service conditions, which different from the independent supervisory authorities that operate under GDPR. The debate about regulatory independence stems from this specific institutional design.

The enforcement creditability requires both statutory powers and institutional independence together with transparent operational processes. The Board establishes regulatory trust through its independent operations and technical knowledge. The executive branch holds appointment authority, which creates doubt about its capacity to maintain impartiality.

4.8 Penalty Framework

The DPDP Act establishes major monetary penalties which include fines that reach up to ₹250

crore based on the severity of different offenses. The current situation shows a major increase from the previous IT Act enforcement system.

The penalty schedule exists to discourage violations while showing authorities' commitment to enforce the law. The system needs to implement its rules consistently while maintaining fair procedures to create effective deterrent effects.

The Act fails to establish statutory compensation systems that match the standards of various international compensation frameworks. The regulatory system uses penalties for its purposes but needs additional remedies to address specific harm to individuals.

4.9 Cross-Border Data Transfers

The DPDP Act establishes a notification-based system which replaces the previous drafts that focused on data localization requirements. The Central Government allows cross-border transfers to destinations that it designates through official notifications.

The model provides increased flexibility which enables international digital commerce to operate more effectively. The lack of specific adequacy guidelines prevents organizations from determining which data protection practices meet international standards.

The success of this method will need to establish open notification systems which should follow worldwide standards for best practices.

4.10 Structural Balance and Design Philosophy

The DPDP Act reflects a legislative attempt to balance three competing imperatives:

1. Protection of individual privacy;
2. Facilitation of digital innovation;
3. Preservation of sovereign regulatory authority.

The simplified drafting process of the document makes it easier for administrators to understand its contents but the document's structural design choices about exemptions and institutional independence create problems which determine its constitutional strength.

The DPDP Act evaluation in this section uses constitutional proportionality and structural

safeguards as assessment criteria.

5. Constitutional Critique and Proportionality Analysis

The DPDP Act needs to confirm its constitutional standards through Justice K.S. Puttaswamy v. Union of India. The proportionality doctrine requires that any infringement of privacy must satisfy three requirements which include establishing legal grounds and showing valid objectives and proving essential need and conducting proper assessment.

5.1 Government Exemptions

The Central Government possesses authority to exempt specific agencies from the Act through Section 17 when it needs to safeguard State sovereignty and State security and public order needs. The exemption clause presents proportionality issues because it extends beyond what the Constitution allows.

The absence of narrowly tailored procedural safeguards or mandatory independent review mechanisms may permit expansive executive interpretation. The balancing test of proportionality requires that any interference must remain less than the advantages which show expected results. The constitutional balance will face disruption through blanket exemptions which contain broad language.

Judicial scrutiny will therefore be critical in ensuring that exemptions remain exceptional rather than routine.

5.2 Institutional Independence

The DPDP Act grants the Central Government control over appointing members and establishing work conditions for the Data Protection Board, which operates independently according to the GDPR. The regulatory body needs structural safeguards because administrative oversight of its operations does not fully eliminate its independence.

The public will lose trust in the regulatory system if people see the enforcement body as controlled by executive power. Institutional design is thus central to constitutional compliance.

5.3 Limited Remedial Framework

The Act establishes severe penalties for non-compliance activities yet fails to provide a clear

compensation method through which affected persons can obtain recompense. Data misuse protection must establish a rights-based system that delivers effective solutions to individuals who suffer from data misuse.

The enforcement system will give preference to regulatory penalties instead of providing individual compensation because it lacks accessible compensation pathways.

6. Comparative Perspective: Global Convergence and Divergence

The European Union's GDPR establishes the most powerful international standard for protecting personal data. The system requires organizations to prove their data protection efforts, while it limits data collection to necessary information and grants users data portability rights and establishes independent monitoring bodies.

The DPDP Act establishes a simplified system which allows organizations to operate with greater flexibility than the previous model. The system requires organizations to obtain user consent for data processing and to inform users about security breaches, but it does not provide users with advanced rights which include data portability and impact assessment frameworks.

The GDPR links penalty costs to international business income which creates a stronger deterrent effect against multinational companies. The Indian penalty system imposes significant financial penalties on organizations, but these penalties remain bound by predefined legal restrictions.

The Indian system follows its actual cultural situation. The strict rules of a regulatory framework will create excessive compliance demands which will hinder the progress of start-ups in a developing digital market. The DPDP Act functions as an effective solution which protects personal information while supporting business expansion.

The two systems establish different regulatory approaches which result in two opposing methods: rights-maximalist and innovation-compatible governance.

7. Implementation and Future Challenges

The enforcement ability of the DPC Act will largely depend on the administrative and procedural capacity put into implementation.

7.1 Regulatory Capacity

The Data Protection Board needs to establish its technical capabilities and transparent procedural operations and its ability to apply regulations consistently. The institutional framework needs to be improved before statutory rights can become more than mere declarations.

7.2 Digital Literacy

Public awareness serves as the essential requirement for people to exercise their rights. The country needs digital grievance systems and easy-to-understand notices because its citizens have different levels of digital skills.

7.3 Startup Compliance

Large corporations possess resources which enable them to establish compliance frameworks while smaller businesses encounter difficulties during their transition period. The required enforcement methods should match the level of innovation protection needs to maintain research development activities.

7.4 Emerging Technologies

The Act does not provide complete solutions to the challenges which artificial intelligence and biometric authentication and automated decision-making systems present. Future changes to the law or its regulations will need to establish criteria for assessing algorithmic accountability.

8. Conclusion

The Digital Personal Data Protection Act 2023 brings a revolutionary change to India's digital constitutionalism through its implementation. The law establishes a regulatory framework for digital personal data which derives from the recognition of privacy as a fundamental right.

The Act achieves its strengths through three elements, which include its consent-based system and its defined data fiduciary responsibilities and its established enforcement systems and its major penalty structure. India shows its dedication to international data handling practices through this initiative.

Structural issues continue to exist in the system. The Data Protection Board received limited protection from institutional safeguards which resulted from broad governmental exemptions and the system lacked precise rules for delivering compensation to victims. The Puttaswamy case established a proportionality standard which must direct all future legal interpretation and enforcement activities.

To strengthen the framework, the following reforms may be considered:

- Narrowly tailored exemption provisions with mandatory review safeguards.
- Greater institutional independence for the Data Protection Board.
- Clear statutory compensation mechanisms for affected individuals.
- Detailed subordinate legislation addressing emerging technologies.

The DPDP Act will achieve its long-term success through three essential elements which include its legal framework and its proper implementation and active judicial monitoring and institutional structure. The protection of individual privacy rights in a democracy which is becoming increasingly digital must remain an essential principle of constitutional governance.

FOOTNOTES -

1. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
2. Information Technology Act, No. 21 of 2000, § 43A, India Code (2000).
3. Puttaswamy, (2017) 10 S.C.C. at 1.
4. Digital Personal Data Protection Act, No. 22 of 2023, § 3, India Code (2023).
5. Id. § 6.
6. Id. § 7.
7. Id. § 16.
8. Id. § 17.
9. Kharak Singh v. State of Uttar Pradesh, A.I.R. 1963 S.C. 1295 (India).
10. Govind v. State of Madhya Pradesh, (1975) 2 S.C.C. 148 (India).
11. People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 S.C.C. 301 (India).
12. Justice B.N. Srikrishna Committee, Ministry of Electronics & Information Technology, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018).
13. Personal Data Protection Bill, 2019, Bill No. 373 of 2019 (India).
14. Digital Personal Data Protection Act, No. 22 of 2023, pmbl., India Code (2023).
15. Id. § 2(t).
16. Id. § 2(i).
17. Id. § 2(j).

18. Id. § 8.

19. Id. § 9.

20. Id. § 10.

21. Id. § 11.

22. Id. § 12.

23. Id. § 13.

24. Id. § 14.

25. Id. § 18.

26. Id. sched.

27. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).

28. Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1.

29. Id. art. 5.

30. Id. art. 44.

31. Organisation for Economic Co-operation and Development (OECD), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013).

32. U.N. Human Rights Council, The Right to Privacy in the Digital Age, G.A. Res. 68/167 (Dec. 18, 2013).

33. Gautam Bhatia, The Transformative Constitution and Privacy After Puttaswamy, 8 NUJS L. Rev. 1 (2018).

34. Apar Gupta & Raman Jit Singh Chima, India's Data Protection Landscape After the DPDP Act, 5 Indian J.L. & Tech. 45 (2023).

35. Ministry of Electronics & Information Technology, Government of India, Explanatory Note on the Digital Personal Data Protection Act, 2023 (2023).

36. Aadhaar (Justice K.S. Puttaswamy) v. Union of India, (2019) 1 S.C.C. 1 (India).

37. Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).

38. Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India).

39. Constitution of India, art. 21.

40. Constitution of India, art. 19(1)(a).

41. Constitution of India, art. 14.

42. Digital Personal Data Protection Act, No. 22 of 2023, § 4, India Code (2023).

43. Id. § 5.

44. Id. § 6(4).

45. Id. § 8(5).

46. Id. § 15.

47. Id. § 19.

48. Id. § 20.

49. Id. § 22.

50. Regulation (EU) 2016/679 art. 20, 2016 O.J. (L 119) 1.

51. Id. art. 52.

52. Id. art. 83.

53. Lee A. Bygrave, Data Privacy Law: An International Perspective 45–62 (Oxford Univ. Press 2014).

54. Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814 (2011).

55. Christopher Kuner, The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, 11 Privacy & Sec. L. Rep. 6 (2012).

56. Orla Lynskey, The Foundations of EU Data Protection Law (Oxford Univ. Press 2015).

57. Justice B.N. Srikrishna Committee, supra note 12, at 22–35.

58. Ministry of Electronics & Information Technology, Government of India, Digital Personal Data Protection Act: Frequently Asked Questions (2023).

59. Gautam Bhatia, Privacy and the Public-Private Divide in India, 8 NUJS L. Rev. 1 (2018).

60. Apar Gupta, India's Data Protection Law: Between Sovereignty and Surveillance, 5 Indian J.L. & Tech. 45 (2023).