A STEP FORWARD? UNPACKING THE GAPS AND GOVERNMENT OVERREACH IN THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Mr Abhishek Tiwari
Graduation: Chanakya National Law University, Patna, Batch of 2024
Post-Graduation: Rajiv Gandhi National Law University, Batch of Patiala 2025
Current Position: Advocate at Delhi High Court

ABSTRACT

After a long wait, India finally has a data privacy law—the Digital Personal Data Protection Act of 2023. This was a huge deal, especially since the Supreme Court already said that our privacy is a fundamental right.

On the surface, the law seems to do the right things. It sets up basic rules for consent and even creates a Data Protection Board to oversee everything. But when you dig a little deeper, you find some serious problems.

The biggest issue? The government basically gave itself a free pass, with exemptions so broad they could lead to unchecked surveillance. Plus, compared to powerful privacy laws like Europe's GDPR, the enforcement mechanisms here are pretty weak, and some of the key rules are frustratingly vague.

So, what's the bottom line? The DPDP Act is a necessary first step, but it feels like a shaky one. To actually protect citizens in this digital age, it needs major fixes—starting with closing those government loopholes and giving the law some real teeth.

1. Introduction

Protecting personal information has become crucial in today's digitally connected world.[1] The project delves into importance, difficulties, and changing environment with respect to digital data protection. The field of digital personal data protection is complex and includes ethical, technological, and legal aspects.[2] Its main goal is to protect people's personal information misuse and illegal access. It is impossible to overestimate the significance of protecting digital personal data. Large volumes of personal data are gathered, processed, and stored by organizations and entities as a result of people's growing online activity. Research, service customisation, and corporate operations all benefit greatly from this information. [3]

It is still a delicate task to strike a balance between the legitimate objectives of law enforcement, corporations, and individuals' right to privacy. Additionally, new technologies like big data analytics, artificial intelligence, and the Internet of Things (I0T) add new complexity to the data protection landscape. Finding the ideal balance between privacy and innovation will be constant struggle.[4] In our digital world, protecting digital personal data is crucial. In a world that is becoming more and more data-driven, it is essential to protecting people's privacy, trust, and autonomy. Maintaining a safe and private online environment will continue to depend on addressing the difficulties and moral dilemmas related to data protection.

India's path to strong data protection laws began with the Information Technology Act, 2000 (IT Act)[5] and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (SPDI Rules)[6]. Although these laws offered some protection, they were not enough to handle the growing complexity of data privacy in the digital age. The Supreme Court of India's landmark 2017 decision in Justice K. S. Puttaswamy v. Union of India[7] made clear the need for comprehensive data protection laws after the court acknowledged the principle of privacy.

---

[1] "Daniel J. Solove, Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880 (2013).
[2] 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).
[3] Mamtaben Danabhai Patel, *A Study on Digital Personal Data Protection Act, 2023*, 11 Int'l J. Rsch. in all Subjects in all Multi Langs. 1 (2023).
[4] *Ibid"*
[5] *The Information Technology Act, 2000*, No. 21 of 2000, India Code (2000).
[6] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
[7] Supra note 5

But India still lacked a data protection law comparable to the General Data Protection Regulation (GDPR) of the European Union,[8] which established a global standard for data privacy. With several drafts of the proposed data protection bill being published over the years, India's efforts to create a stand-alone data protection law started in earnest in 2018. Ultimately, the DPDP Act became a law in 2023 after being accepted by both chambers of the Indian Parliament and receiving the president's approval. An important turning point in India's data protection history was reached with this.[9]

With the passage of the Digital Personal Data Protection Act, 2023 (DPDP Act)[10], India has made a major step in guaranteeing data protection and privacy in an era characterized by the unparalleled development and use of digital personal data. In a fast-changing digital landscape, this comprehensive legislation aims to address the complexities and issues related to data privacy.[11] The DPDP Act expands on earlier data protection initiatives in India by offering a legislative framework designed to protect data principals' rights and interests while laying out explicit duties for data fiduciaries.[12]

2. CONCEPTUAL FRAMEWORK OF DIGITAL PERSONAL DATA PROTECTION

Definition: Protecting the data and private information that people create and share in digital contexts is the primary goal of digital personal data protection. Controlling how entities and organizations collect, store, process, and distribute this data is its aim.[13]

Scope: The breadth of this idea is more limited than that of the right to privacy. Its main focus is on safeguarding personally identifiable information (PII) in digital contexts, including names, addresses, financial data, online activity, and other data.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.
[9] Press Release, Ministry of Elecs. & Info. Tech., The Digital Personal Data Protection Act 2023 (Aug. 11, 2023), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023
[10] The Digital Personal Data Protection Act, No. 22 of 2023, (2023).
[11] World Economic Forum, Data Free Flow with Trust (DFFT): Paths Towards Free and Trusted Data Flows (2020), https://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf
[12] *Id*
[13] Regulation (EU) 2016/679, art. 5(1)(b), 2016 O.J. (L 119) 1, 35. (requiring data to be collected and processed lawfully, fairly, and transparently).

Challenges:

The fast development of technology and data-driven enterprises makes it difficult to ensure appropriate digital personal data protection.[14] It can be difficult to strike a balance between protecting data and legitimate company interests, legal requirements, and individual rights.[15]

3. Evolution and development of data protection laws in india

3.1 History of data protection laws in India

To understand the significance of the DPDP Act, it is essential to examine the historical evolution of data protection laws in India. This section provides an overview of the key legislations and rules that preceded the DPDP Act and identifies their limitations.

3.1.1 The Information Technology Act, 2000 (IT Act)

The IT Act[16], enacted in 2000, was India's first attempt to regulate various aspects of electronic commerce and digital transactions. While it contained provisions related to data protection and security, it primarily focused on issues such as digital signatures, cybercrime, and electronic records. The IT Act introduced Section 43A[17], which dealt with compensation for failure to protect sensitive personal data.

3.1.2 The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (SPDI Rules)

To enhance the data protection provisions of the IT Act, the Indian government enacted the SPDI Rules in 2011.[18] These regulations sought to give businesses a framework for putting "reasonable security practices and procedures" into place in order to safeguard private

[14] Supra note 1
[15] Omer Tene & Jules Polonetsky, Privacy in the Age of Big Data: A Legal and Ethical Analysis, 65 STAN. L. REV. 1375, 1380 (2013).
[16] Supra note 8
[17] The Information Technology Act, 2000, No. 21 of 2000, § 43A, India Code (2000) & KHAITAN & CO, DATA PROTECTION IN INDIA: AN OVERVIEW (2021), https://www.khaitanco.com/sites/default/files/2021-04/Data%20Protection%20in%20India%20Overview.pdf.
[18] Vipul Kharbanda & Cheshta Arora, *Guidelines to Build Robust Security Standards for the Financial Technology Sector in India*, 18 IND. J.L. & TECH. 1 (2022).

information.[19] According to the regulations, organizations that collected and processed sensitive personal data had to have data subjects' consent and follow certain data protection guidelines.

Although the SPDI Rules were a positive step for data security, they did not fully address more general data privacy issues; instead, they concentrated largely on protecting sensitive personal data. Furthermore, their efficacy was constrained by the absence of a specialized data protection authority and enforcement procedures.[20]

3.2. Need for the data protection of law

3.2.1 Limitations of Previous Laws

Although significant in and of themselves, the IT Act and SPDI Rules have a number of drawbacks.

a. Lack of Comprehensive Coverage: These laws mainly addressed sensitive personal data and did not offer a comprehensive framework for data protection that covered all types of personal data.[21]

b. Ambiguity: Organizations were uncertain about how to ensure data protection because the legal framework was unclear about compliance requirements.

c. Enforcement Difficulties[22]: Efficient implementation and supervision were impeded by the lack of a specific data protection authority and well-defined enforcement procedures

At first glance, India's data protection law might appear similar in scope to the data protection framework in the United States, given its application to specific industries and target audiences. However, a key difference lies in their focus: U.S. data protection laws are predominantly designed to shield individuals from state interference and often exclude the private sector from

[19] Sudhanwa Sandeep, *The SPDI Rules: An Early Attempt at Data Protection in India and its Limitations*, 4 IND. J.L. & LEGAL RSCH. (2022), https://www.ijllr.com/post/the-spdi-rules-an-early-attempt-at-data-protection-in-india-and-its-limitations.
[20] COMM. OF EXPERTS ON A DATA PROT. FRAMEWORK FOR INDIA, MINISTRY OF ELECS. & INFO. TECH., GOV'T OF INDIA, A FREE AND FAIR DIGITAL ECONOMY: PROTECTING PRIVACY, EMPOWERING INDIANS (2018).
[21] Deborshi Barat, *A Primer on Data Regulation and AI Development in India*, Indian J.L. & Tech. Blog (Nov. 29, 2023), https://www.ijlt.in/post/a-primer-on-data-regulation-and-ai-development-in-india
[22] *Id*

their purview. In contrast, India's approach makes no such distinction. Its data protection framework is driven by the overarching goal of safeguarding data itself, applying equally to both public and private entities.

There are no particular laws in India that address privacy or data protection; instead, protection is provided by a number of laws pertaining to information technology, intellectual property, contracts, the cyber world, etc.

3.2.2 Right to Privacy and the Challenges of the Digital Age

According to the ruling in *Justice K.S. Puttaswamy (Retd.) v. Union of India (2018*), privacy is a fundamental right under Article 21 that is necessary for liberty, autonomy, and dignity.[23] In digital age protecting privacy has become more essential than ever, as with the proliferation of mobiles, internet connected devices, both government and private players store vast amount of data, including the sensitive information raised serious concerns about privacy protection, as data breaches, unauthorized surveillance, and misuse of personal information have become frequent occurrences, underscoring the need for strong privacy protections.[24].

Different data types face different privacy risks in the digital age.[25]Strong security measures are necessary to prevent the misuse of **personal data**, such as names, contacts, and photographs. **Financial data** which include information related to banking and transaction also needs a high security as it is extremely vulnerable to fraud risks. **Health data**, which includes information such as medical and biometric records, requires protection to maintain confidentiality and avoid discrimination. **Meta Data,** these are the data which is not directly identifiable, but they contain essential information on person's behavior and interests [26]

3.3 The Digital Personal Data Protection Act, 2023: -

The Digital Personal Data Protection Bill, 2023 was introduced by the Minister of Electronics & Information Technology on August 3, 2023, and was passed by the Lok Sabha on August 7,

[23] *Justice K. S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1.
[24] Parkhi Agarwal, *Constitutional Right To Privacy in Relation to Technology and Data Collection Practices*, AK LEGAL (July 27, 2023), https://aklegal.in/constitutional-right-to-privacy-in-relation-to-technology-and-data-collection-practice
[25] Supra Note 15
[26] ANN CAVOUKIAN & DANIEL ROSENBERG, INFO. & PRIVACY COMM'R OF ONT., METADATA SURVEILLANCE: A PRIMER (2014), https://www.ipc.on.ca/sites/default/files/legacy/Resources/metadata.pdf.

2023. The measure was unanimously approved by the Rajya Sabha on August 9, 2023, and the President signed it into law on August 11, 2023.[27]

The principal purpose of the act is to develop a robust framework for the processing and protection of personal data.[28] Both the processing of personal data in India, including both online and digital offline data, and the processing of personal data outside of India related to the delivery of goods or services in India will be covered by the Act. The Act also creates the foundation for several other laws, such as the Digital India Act and other sector-specific privacy and data protection laws, to help India push forward with the adoption of AI and other advanced technologies while protecting personal information.

However, it is believed that a number of implementation-related matters need to be clarified, which could happen if the Data Protection Board of India is established and rules under the Act are published. The Act as a whole, enhanced by lengthy post-draft consultations, represents India's distinct position on contemporary data protection. Although the Act's rules are not as comprehensive as those of the EU's GDPR, it does require a substantial change in the way Indian companies now handle privacy and personal data, and it gives CG the legal authority to manage, keep, and keep an eye on the personal data of its residents.

3.4 Key features of the Digital Personal Data Protection Act, 2023

The scope, breadth, and requirements of the DPDP Act differ significantly from those of its predecessors. This section highlights the essential components of the DPDP Act and offers a thorough examination of its main clauses.

3.4.1 Applicability and Scope

There are two situations in which the DPDP Act regulates the handling of digital personal data in India:

4 When such information is gathered digitally from data principals.

5 When non-digital data is first gathered and then converted to digital form.

[27] Supra Note 9
[28] Daniel J. Solove, *Understanding Privacy* 1 (Harv. Univ. Press 2008).

This more focused approach sets the DPDP Act apart from the 2022 Bill and clarifies that processing personal data in a non-digitized format is not included.[29] The goal of this expanded scope is to address data privacy issues unique to digital platforms.

Additionally, if the processing of digital personal data is related to the delivery of goods or services to data principals situated in India, the DPDP Act expands its jurisdiction beyond India's boundaries.

The DPDP Act takes a more comprehensive approach than the GDPR, which mainly targets those who are physically present in the EU or who are EU citizens.[30] However, the Act leaves opportunity for interpretation and future regulatory guidance because it does not specifically address its relevance to the processing of personal data pertaining to data principals located outside of India. [31]

3.4.2. Exemptions for Startups and Transitory Provisions

The DPDP Act includes provisions for possible startup exclusions in recognition of the particular difficulties experienced by entrepreneurs.[32] These customized solutions seek to strike a compromise between the need to help new enterprises and encourage innovation while also protecting data. Additionally, the Act preserves exemptions for the state, its agencies, and for statistics and research purposes.

3.4.3. Personal Data

The term "digital personal data," which refers to "personal data" supplied in digital form, is introduced by the DPDP Act.[33] This differentiation aids in elucidating the extent of the Act and sets it apart from non-digital personal data. The DPDP Act defines "personal data" as "any data pertaining to an identifiable individual," in contrast to its predecessors. Importantly,

---

[29] Internet Freedom Found., *IFF's First Read of the Draft Digital Personal Data Protection Bill, 2023* (July 5, 2023), https://internetfreedom.in/iffs-first-read-of-the-draft-digital-personal-data-protection-bill-2023/.
[30] Vinod Joseph & Ira A. Eddi, *The Digital Personal Data Protection Bill, 2022 – An Analysis*, MONDAQ (June 12, 2023), https://www.mondaq.com/india/data-protection/1326224/the-digital-personal-data-protection-bill-2022--an-analysis.
[31] Anirudh Burman, *Understanding India's New Data Protection Law*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Oct. 12, 2023), https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law.
[32] Latham & Watkins, *India's Digital Personal Data Protection Act, 2023 vs. The GDPR: A Comparison* (2023), https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf.
[33] Supra Note 10

the DPDP Act does not include the distinction between "sensitive personal data" and "critical personal data," which was included in earlier iterations. This change represents a break from the prior paradigm and is worth considering further in light of its potential effects on privacy and data protection issues.

The DPDP Act requires data fiduciaries to protect the personal information under their control by putting "reasonable security measures" in place to stop breaches.[34] Data fiduciaries must notify the impacted data principals and the Data Protection Board in the case of a data breach. The precise definition of "reasonable security measures" is left open to interpretation by the Act, nevertheless.[35] Nevertheless, there are severe consequences for noncompliance that leads to a compromise of personal data.

3.4.4. Processing of Personal Data

The DPDP Act carefully defines what constitutes "processing," which includes a broad variety of actions taken on digital personal data. Collection, recording, organization, storage, retrieval, use, sharing, and more are all included in this thorough definition. Processing also includes actions like data limitation, erasure, and destruction.

The Act adds clauses requiring verifiable parental consent for the processing of children's personal data. It does not, however, provide a clear definition of "verifiable" consent, which could lead to ambiguity and implementation issues.[36] By decreasing the age threshold for parental consent, the Act gives the Central Government the power to exclude some data fiduciaries from this obligation, so long as the processing is judged safe. Data fiduciaries must also refrain from processing personal information that can have a negative impact on well-being of a child. The DPDP Act allows personal data to be transferred to nations outside of India, unless the Central Government specifically prohibits it. This clause preserves the government's power to control cross-border data transfers when required while acknowledging the global nature of data flows.

3.4.5. Significant Data Fiduciaries

The Central Government may designate specific data fiduciaries or groups of them as

[34] Supra Note 44
[35] Supra Note 43
[36] Supra note 46

"significant data fiduciaries" under the DPDP Act. Numerous criteria, such as data volume, sensitivity, risk to data principles, electoral democracy, and state security, are used to determine this classification. Other criteria, such "other factors," that were included in earlier drafts are not specified in the Act.[37]

Additional responsibilities for significant data fiduciaries include hiring a data protection officer, working with an outside data auditor, performing impact analyses on data security, and going through regular compliance audits. Penalties for noncompliance with these responsibilities can be severe and can reach INR 250 crore.[38]

3.4.6. Consent

a. Data Fiduciary

Data fiduciaries are only permitted to process personal data for legitimate reasons under the DPDP Act, provided that consent is obtained.[39] Free, explicit, informed, unconditional, and unambiguous consent is required. To express consent to the processing of their personal data for the designated and required purpose, the data principal must take a clear affirmative action. The consent request needs to be presented in an easy-to-understand format with the ability to view it in several languages. In order to handle correspondence from data principals, data fiduciaries must also give the data protection officer or an authorized representative their contact information.

Additionally, data fiduciaries must give data principals a thorough notice before requesting consent. An explanation of the personal information to be gathered, the reason for its processing, the rights of the data principal, and information on how to lodge a complaint with the Data Protection Board should all be included in this notice.[40] When consent was granted prior to the DPDP Act's passage, data fiduciaries are obligated to deliver the necessary notice "as soon as it is reasonably practicable."

[37] Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2nd ed. 2021)
[38] *Supra Note 10*
[39] Ibid
[40] Yogen Vaidya & Raghav Jain, *India's Digital Data Protection Bill: Implications of "Deemed Consent"*, ERNST & YOUNG (Jan. 25, 2023), https://www.ey.com/en_in/insights/cybersecurity/india-s-digital-data-protection-bill-implications-of-deemed-consent.

b. Data Principals

Data principals can use a "consent manager" to give, manage, review, or revoke their consent. These consent managers, who are registered with the Data Protection Board, provide clear and easily accessible consent management platforms. The precise responsibilities and functions of consent managers are yet unknown, though, which raises concerns regarding their efficacy and execution.

Data fiduciaries and their processors must erase and stop processing the personal data upon withdrawal, unless retention is mandated by applicable laws. The DPDP Act introduces the concept of "consent of the parent," which includes the consent of a lawful guardian where applicable, especially in cases involving data processing related to children

c. Parental Consent

Data principals retain the right to withdraw consent at any time, and this withdrawal does not affect the legality of prior data processing based on consent.

3.4.7. Data Protection Board of India[41]:

In accordance with Chapter V of the Act, CG is required to form a Data Protection Board of India (Board) with a chairperson and other members. The Board will exercise and carry out the duties and responsibilities outlined in Sections 27 and 28 of the Act, which include, among other things,

(i) ordering immediate corrective or mitigation actions in the event that Personal Data is compromised,

(ii) looking into the breach, and

(iii) applying sanctions in accordance with the Act.

[41] Supra note 10

Section 39 prohibits any other civil court from hearing a suit or procedure pertaining to any matter that the Board has the authority to decide under the Act.[42] The Board will be a civil court with original jurisdiction to hear complaints or matters pertaining to the Act.

3.4.8. Appeals:

According to Section 29, the Telecommunications Dispute Settlement and Appellate Tribunal (TDSAT), which was founded by the Telecom Regulatory Authority of India Act, 1997 (TRAI Act), would hear appeals against the Board's rulings. The window for filing such an appeal is sixty (60) days from the date the Board's decision was received. Furthermore, in accordance with Section 18 of the TRAI Act, the Hon'ble Supreme Court will hear appeals of the orders issued by TDSAT.[43]

3.4.9. Penalties:

The amount of penalties to be applied for different offenses and violations under the Act is specified in the Schedule to the Act.

For example, a penalty of (i) INR 200 Crore for failing to comply with obligations regarding children; (ii) INR 250 Crore for failing to implement security measures to prevent data breaches, as stipulated in Section 8(5); and (iii) INR 200 Crore for failing to notify the Board or the Data Principal of a breach involving personal data, as stipulated in Section 8(6). Following an investigation under Section 33[44], the Board will impose such fines.

4. Criticism of Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act) is a landmark step towards safeguarding personal data in India's rapidly evolving digital landscape. Critics argue that the Act's definitions lack clarity, its provisions for government exemptions and cross-border data transfers are overly discretionary, and its enforcement mechanisms are inadequate to deter large-scale data breaches. Moreover, the DPDP Act's limited focus on emerging technologies such as artificial intelligence and biometrics leaves critical privacy risks unaddressed. Digital

[42] Pradip Kashyap, *Digital Personal Data Protection Act, 2023: A New Light into the Data Protection and Privacy Law in India*, 2, ICREP Journal of Interdisciplinary studies (2024).
[43] I*d*
[44] *Id*

personal data protection, while essential, has faced criticism and scrutiny for various reasons. Here are some common criticisms of data protection efforts:

4.1. Definitional Issues (Section 2)

Section 2's definitions have drawn criticism for being imprecise, which could cause confusion in interpretation and application. For example, the definition of "harm" in Section 2(12) is too broad and encompasses ambiguous expressions like "reputational harm" and "denial of service."[45]

Furthermore, it is unclear from the word "personal data" if encrypted, derived, or pseudonymized material is included, which may cause data fiduciaries to interpret it differently. Additionally, the idea of "significant data fiduciaries" is not well defined, lacking any precise criteria or boundaries for categorization, which may result in uneven implementation across sectors.

4.2. Data Breach Notification (Section 9)

The lack of urgency in Section 9(4)'s requirement that data fiduciaries notify the Data Protection Board in the event of a data breach is a significant departure from the GDPR, which requires breach notifications within 72 hours (Article 33).[46] Additionally, the Act does not distinguish between minor and major breaches and does not offer specific guidance on notification formats, risk assessments, or content requirements. Lastly, there is no mandatory requirement to notify affected individuals about breaches, which limits transparency and prevents individuals from taking proactive measures to mitigate potential harm.

Although it is a first step towards India's data protection framework, the DPDP Act needs to be greatly improved in order to fill important loopholes. To guarantee strong privacy protection, efficient compliance, and significant recourse for impacted parties, the Act must be in line with international best practices like the GDPR, which are characterized by extensive government exclusions, ambiguous definitions, and lax enforcement mechanisms. For the Act to successfully protect digital privacy in India, these issues must be resolved.

[45] Digital Personal Data Protection Act, No. 22 of 2023, § 2 (India).
[46] Digital Personal Data Protection Act, No. 22 of 2023, § 9(4) (India)

4.3. Ineffectiveness of Regulations:

Critics argue that the DPDP Act's regulatory framework could not be sufficient to fully address privacy infractions and data breaches. Although the Act lays forth data protection principles, businesses that engage in careless or malevolent data practices may not necessarily be strongly discouraged by its enforcement procedures and penalties.

- The DPDP Act's Section 25[47] outlines penalty for non-compliance, which can reach ₹250 crore. However, unlike the GDPR, which levies fines of up to €20 million or 4% of global revenue (Article 83), there are worries that this flat penalty method ignores the extent of harm or the global turnover of giant digital businesses.

- Reactive enforcement, in which infractions are dealt with only after harm has been caused, may result from the absence of clear norms for proactive monitoring and auditing of businesses' data activities.

Although there aren't many significant precedents under the DPDP Act in India, cases like Cambridge Analytica (UK)[48] show how weak enforcement can make privacy violations worse. In some jurisdictions, tech companies were able to misuse personal data without incurring significant penalties

4.4. Emerging Technologies and their Challenges:

Critics point to the DPDP Act's lack of vision in tackling the problems presented by cutting-edge technology like biometrics, artificial intelligence (AI), and quantum computing. These technologies pose particular risks, such as:

I. The potential misuse of biometric data, like facial recognition, for unauthorized surveillance or identity theft;

II. The absence of specific provisions for automated decision-making, which may affect data

[47] Digital Personal Data Protection Act, No. 22 of 2023,§. 25 (India)
[48] Info. Comm'r's Off., Investigation into the Use of Data Analytics in Political Campaigns (Nov. 6, 2018), https://ico.org.uk/media2/migrated/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

principals' rights;

III. Profiling and behavioural tracking, which are common in AI systems and can result in discriminatory outcomes.

There are gaps in oversight for cutting-edge data applications because the DPDP Act does not specifically provide safeguards for automated decision-making and profiling, unlike the GDPR, which addresses these cases under Article 22. Section 4 describes the general principles of processing but does not go into regulating advanced technologies like AI.

- **Challenges**:

As seen by international incidents like Clearview AI (USA)[49], where face recognition technology was used for mass monitoring, creating serious privacy issues, the lack of specific regulations for developing technologies could result in regulatory uncertainty and possible harm.

4.5. Government Intervention

The Central Government is given discretionary rights by the Act, including the ability to categorize important data fiduciaries. There may be worries about possible government meddling in data protection issues as a result of this discretionary power. It will be essential to strike the correct balance between business liberty and regulatory scrutiny. Although the Act's current version appears to protect personal data, there may be issues with how the requirements are practically implemented.

For example, Section 36 gives the Central Government the authority to request "such information" from the Board or any Data Fiduciary or intermediary as it sees fit. When examined through a legislative perspective, such broad vocabulary and extensive power would demonstrate the Central Government's long-standing desire to monitor.

Furthermore, Section 17(2)(a) gives the CG the authority to exclude any State instrumentality from the strictures of the laws pertaining to the processing of personal data.[50]

[49] *ACLU v. Clearview AI, Inc.*, No. 2020-CH-04353 (Ill. Cir. Ct. May 28, 2020).
[50] Digital Personal Data Protection Act, 2023, No. 22, §§ 17(2)(a), 36 (India).

Furthermore, the RTI Act's balance between privacy and informational rights will be lost because Section 44(3) of the Act amends Section 8(1)(j) of the Right to Information Act, 2005 (RTI Act). This is because the authority of a Public Information Officer (PIO) has been expanded, allowing them to deny an application submitted under the RTI Act on the grounds that the information requested pertains to personal data.

4.6. Enforcement Mechanisms

A key component of the DPDP Act is the creation of the Data Protection Board of India (Section 19) as the main regulatory body. However, the Board's operational independence, resources, and transparency are critical to its effectiveness.

Concerns: -

- A single centralized authority may not be able to manage the scope and complexity of data protection issues in a diverse nation like India, according to critics.

- Limited Redressal Mechanisms: Although the Board handles complaints, the absence of provisions for local supervisory bodies (akin to the GDPR's decentralized system under Article 51) may make it more difficult for people in rural areas to access the Board.

- Judicial Oversight: Fairness and accountability issues may arise if there are unclear rules for judicial review of the Board's judgments.

The Supreme Court of India stressed the significance of a strong data protection regime in Justice K.S. Puttaswamy v. Union of India (2017)[51] in order to preserve the basic right to privacy. Critics fear that the Board's limited independence and authority may not be entirely consistent with the values outlined in the ruling.

4.7. Consent Management

To guarantee their efficacy in managing and rescinding consent, the notion of consent managers, which was introduced in the Act, needs more explanation. The ability of data principals to manage their data may be impacted by ambiguities in this area. Before processing children's data, 2023 data fiduciaries are required by Section 9 of the DPDP to get parents' or

[51] Supra note 5

guardians' verifiable consent. Ad targeting for children and damaging data processing are also prohibited by the Act. However, certain organizations, such as healthcare and educational institutions, may be exempt from age gating regulations and the need for verifiable parental agreement. Additionally, based on the particular reason they must treat a child's data, certain entities may be excused from the rules on a limited basis.

- **Issues:**

I. Although the statute establishes safeguards for kid data, such as parental consent, issues with age verification and determining what constitutes harm to children still exist.

II. Careful handling is necessary when parents withdraw their consent or when youngsters attain the legal age of consent.

III. Implementation challenges may arise from things like storing biometric data and guaranteeing compatibility across multiple devices.

IV. One of the main issues facing the business is that the legislation itself makes no recommendations about how platforms can implement age-gating.

V. How to accurately create a child's relationship with his or her parents is another difficulty.

The primary cause of the delay in the release of the data protection regulations, which are necessary for the DPDP Act to be operationalized, is the inability to reach a definitive decision regarding the verifiable parental consent provision. The Act's modalities depend on at least 25 of these provisions.

- **Likely Solution and Their Limitations:**

a. The MeitY first thought about using the Aadhaar-reliant Digi Locker app for parents. However, it was rejected due to privacy and scalability issues.

b. Another choice was for the sector to develop a government-approved electronic token system. But there were also real-world drawbacks to this strategy.

c. The representatives of the industry proposed a risk-based grading system in a recent meeting with the MeitY, referencing the Age-Appropriate Design Code (AADC) in the UK as

an example.

4.8. Government Exemptions

The Central Government has broad authority under Section 17 of the DPDP Act, which allows it to exempt any government agency from any or all of the Act's obligations. The government may provide such exclusions under Section 17(1) in the name of "public good," "public interest," "national security," or other nebulously defined goals. Critics contend that these phrases' ambiguity poses serious risks of abuse or arbitrary application. For example, the wide notion of "public interest" may be used to excuse surveillance operations or exempt organizations engaged in dubious data methods. Moreover, there are no oversight procedures in place for the exemptions process. Without independent review, public consultation, or parliamentary approval, exemptions can be granted through straightforward government notices.

The DPDP Act does not outline such protections, in contrast to GDPR Article 23, which requires that exemptions adhere to fundamental privacy rights and be subject to stringent proportionality and necessity testing. The potential of long-term abuse is increased when approved exemptions are not subject to frequent evaluations. The GDPR, on the other hand, makes sure that exemptions are routinely reviewed to verify their necessity. Concerns are also raised by Section 17(2), which permits exemptions for statistical, archival, and research reasons. Such exclusions could be utilized to avoid compliance under the pretence of acceptable reasons if they lack clear definitions and bounds.[52]

Global instances like as the PRISM surveillance program (USA)[53], where a lack of accountability measures resulted in widespread privacy violations, demonstrate the potential for abuse of exclusions. The right to privacy, which was upheld as a basic right in Justice K.S. Puttaswamy v. Union of India (2017), may be threatened by comparable situations under Section 17 in India, according to critics.

[52] Digital Personal Data Protection Act, No. 22 of 2023, § 17(1), 17(2) (India)
[53] Ewen MacAskill & Gabriel Dance, *What the revelations mean for you*, *in* NSA files decoded: Edward Snowden's surveillance revelations explained, The Guardian (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

4.9. Data Localization and Cross-Border Transfers

Cross-border data transfers are governed by Section 16, which allows transfers to nations and territories that the Central Government notifies. The Act does not, however, specify any particular standards or guidelines for identifying these "notified" nations. This ambiguity casts doubt on the decision-making process's impartiality and transparency, especially when working with countries that might not have strong data protection laws.

The DPDP Act lacks such comprehensive requirements, in contrast to the GDPR's Articles 44–47, which set up a strict adequacy assessment system for cross-border data transfers. According to the GDPR, third countries must exhibit sufficient data protection standards through thorough evaluations that take into account their legal frameworks, enforcement strategies, and judicial remedies. Transfers to nations with inadequate or non-existent data are nevertheless possible because the DPDP Act lacks such requirements.[54]

The absence of a data localization requirement for important personal data is another source of dispute. The final version of the Act has weakened the stricter localization requirements included in earlier drafts. This may make it easier for global corporations to conduct business, but it also raises questions about India's capacity to successfully enforce its laws in the event of data breaches or disputes in other countries.

Consequences:

As demonstrated in cases such as Schrems II (CJEU, 2020)[55], where cross-border data transfers from the EU to the US were declared illegal due to insufficient protection against surveillance, the lack of strict localization and transfer measures might result in jurisdictional issues. In the absence of strong frameworks, India would encounter comparable difficulties in guaranteeing responsibility for data breaches that take place elsewhere.

4.10. Data Protection Board Structure

The primary authority for implementing data protection regulations is the Data Protection Board of India (DPBI), which was founded in accordance with Section 19. However, there are serious questions about its independence and impartiality raised by its appointment

[54] Council Regulation 2016/679, arts. 44–47, 2016 O.J. (L 119) 1 (General Data Protection Regulation).
[55] Case C-311/18, *Data Prot. Comm'r v. Facebook Ir. Ltd.* (Schrems II), ECLI:EU:C:2020:559 (July 16, 2020).

procedure and institutional makeup. There are no legal safeguards guaranteeing the Board's independence, and it is wholly selected by the government.

The lack of particular qualifications for Board members is a point of contention. The Data Protection Board of India does not impose the same standards as the GDPR, which guarantees that supervisory authorities are made up of people with the necessary technical, legal, and privacy skills. Additionally, important stakeholders like the court, civil society, and technical specialists are not represented, which raises concerns about bureaucratic domination and possible conflicts of interest.

The Board's perceived independence and neutrality are compromised by the government's exclusive authority over the selection and removal process. The supervisory authorities under the GDPR, on the other hand, are set up to operate without interference from the government and have explicit measures in place to avoid conflicts of interest.

Consequences:

In the absence of sufficient protections, the Data Protection Board of India runs the risk of becoming a weak regulator that cannot hold public or private organizations responsible. In nations like the UK, where the Information Commissioner's Office (ICO) has shown how crucial independence is to efficient oversight and enforcement, lessons can be learned.

4.11. Penalties and enforcement

According to Section 25 of the DPDP Act, non-compliance carries monetary penalties of up to ₹250 crore. Although this seems substantial, it is thought to be insufficient in comparison to the GDPR's provision for fines 0f up to €20 million 0r 4% of worldwide sales (Article 83), whichever is larger. A fine of ₹250 crore might not be enough of a deterrence for big multinational firms given their earnings. Affected data principals are left without adequate remedies since Section 26 noticeably does not offer individual compensation in circumstances of data breaches or violations. [56]

On the other hand, data subjects have the right to demand direct compensation from controllers or processors for both material and non-material damages under Article 82 of the GDPR. [57]The

[56] Digital Personal Data Protection Act, No. 22 of 2023, § 25, 27(India)
[57] Council Regulation 2016/679, arts. 82-83, 2016 O.J. (L 119) 1 (General Data Protection Regulation).

lack of teeth in the enforcement procedures described in Section 27 is another point of criticism. The Board's capacity to identify and aggressively manage non-compliance is hampered by the lack of search and seizure authority, dawn raids, and strong investigative capabilities.

Challenges:

Regulators in other jurisdictions have encountered similar problems with limited investigative capabilities impeding effective monitoring, which is reflected in this enforcement capability gap. For instance, computer businesses were able to avoid accountability for privacy violations during the early years of the US Federal Trade Commission due to inadequate enforcement methods.

4.12. Compliance requirements

Data fiduciaries are subject to stringent compliance requirements under the DPDP Act, which could be especially difficult for smaller organizations. While Section 9 requires extensive notification requirements that must include specific information about the collection, processing purposes, and the contact details of the data fiduciary, Section 8 defines general liabilities. Although Section 10 mandates that data fiduciaries put in place sufficient security measures, it does not outline the precise requirements or steps, so businesses are unsure of what is expected of them in terms of compliance. In a similar vein, Section 11 places restrictions on data retention without offering helpful advice regarding exceptions or retention schedules.[58]

Due to their frequent lack of funding, startups, small enterprises, and nonprofit organizations are disproportionately impacted. The standards' vagueness and complexity may hinder innovation and place a heavy operational burden on businesses.

While the DPDP Act marks a significant step in India’s journey toward comprehensive data protection, its limitations expose the challenges of drafting a robust and future-ready legal framework. The lack of clarity in definitions, discretionary powers granted to the government, and inadequate provisions for emerging technologies undermine the Act’s potential to safeguard individual privacy effectively. Additionally, enforcement mechanisms need strengthening to ensure accountability and fairness, particularly for powerful entities

[58]Digital Personal Data Protection Act, No. 22 of 2023, § 8–11 (India)

operating in a globalized economy. Addressing these criticisms requires a multi-stakeholder approach, continuous legislative review, and alignment with international best practices like the GDPR. With thoughtful revisions and proactive implementation, the DPDP Act can evolve into a model legislation that protects personal data, fosters innovation, and strengthens public trust in the digital ecosystem.

4.13. Ineffective protection of Privacy under DPDP Act: -

The recent Act does not fully mitigate the concern over privacy, the data protection board, which is tasked with protecting the privacy is not independent, central government has control over it, the Central Government enjoys wide powers, including exemptions for state bodies, this raises fears of overreach.[59]

5. Conclusion and suggestions

Protecting digital personal data is a cornerstone of modern governance and economic stability. India's DPDP Act, 2023, represents a critical step in building a legislative framework to safeguard individual privacy in our data-driven era.

The law directly addresses growing concerns over data breaches, information misuse, and opaque data processing. It builds on the foundation of the "Right to Privacy," as established in the landmark *Justice K.S. Puttaswamy v. Union of India* case, while also recognizing data's role as a driver of economic innovation.

However, the primary challenge lies in implementation and enforcement. The increasing sophistication of cyberthreats, fueled by the integration of AI, Machine Learning, and IoT technologies, creates new vulnerabilities. These modern risks demand a dynamic and vigilant approach to data security, as traditional methods are no longer sufficient to mitigate them.

The success of the DPDP Act hinges entirely on its effective implementation. While the establishment of the Data Protection Board of India is a positive development, its ultimate effectiveness will depend on its structure and operational capacity to address real-world challenges.

[59]Abhishek Singh & Anusha,*The Digital Personal Data Protection Act, 2023: An Ambitious Government Step Towards Ensuring Its Wide Reach,* 70 Indian J. Pub. Admin. (2024).

Several critical areas currently lack specific regulation, including cross-border data flows and the operationalization of penalties. These ambiguities create legal uncertainty for businesses and must be clarified to ensure the Act functions as intended.

A successful data protection framework requires a multi-stakeholder approach:

- **Industry:** Must integrate "privacy-by-design" principles into their core operations.
- **Government:** Must ensure the laws are practical and enforceable.
- **Civil Society:** Must continue to advocate for transparency and accountability.

Furthermore, public empowerment through digital literacy is crucial for the Act's consent mechanisms to be meaningful. In a country with varying levels of digital access like India, ensuring individuals truly understand the implications of their consent remains a significant hurdle. Achieving a balance between innovation and individual rights requires active collaboration across all these sectors.

Bridging the gap between the law's intent and public understanding requires sustained public education and accessible tools that empower users to manage their data rights effectively.

In the global context, India's DPDP Act must be benchmarked against international standards like the European Union's GDPR. While the GDPR sets a high bar with its comprehensive framework and strict enforcement, India's more flexible approach presents both opportunities and challenges. A key area needing refinement is the management of cross-border data flows to align with the realities of global commerce.

Furthermore, the regulatory impact on India's innovation ecosystem, particularly startups and small enterprises, is a critical concern. To prevent compliance from becoming a barrier to growth, it's essential for the government to establish support systems that help these businesses navigate the new requirements. The goal must be to foster innovation, not stifle it with overly complex regulations.

It is also necessary to investigate how technology facilitates compliance. Data protection procedures can be streamlined, expenses can be decreased, and transparency can be increased by utilizing innovations like AI-driven compliance tools and privacy-enhancing technologies

(PETs). Furthermore, establishing a unified platform for complaints and redress regarding data protection may make the procedure easier for both people and businesses. Ultimately, the implementation of the DPDP Act must remain anchored to the fundamental right to privacy. This right is a matter of human dignity and autonomy, not merely a compliance issue. The Act's core challenge is to ensure that rapid technological advancements do not erode these essential values.

The continued growth of the digital economy presents an opportunity for India to position itself as a leader in ethical data governance. By building a trusted digital ecosystem, the Act can attract foreign investment and enhance India's global standing in technology and innovation.

However, realizing this potential requires a commitment to continuous improvement. The Act's provisions must be consistently refined and adapted to stay ahead of the evolving data protection landscape to ensure its long-term success and relevance.

Recommendations for Strengthening the Act:

1. Increased Explicitness and Detail in Provisions: -

Offer precise definitions and instructions to resolve uncertainties in areas such as consent management.

2. Empowerment of the Data Protection Board: -

Ascertain that the Board has sufficient resources, knowledge, and autonomy to successfully carry out its mandate.

3. Public Awareness and Education: -

Start nationwide initiatives to close the digital literacy gap by informing people of their rights and obligations regarding their data.

4. Assistance for Small and Medium Businesses (SMEs): -

To guarantee widespread adherence, create affordable compliance frameworks suited to smaller companies' requirements.

5. Periodic Review and Adaptation: -

Provide procedures for routine evaluation of the Act's effects to guarantee its ongoing applicability in the face of technological breakthroughs.

In essence, the DPDP Act of 2023 signifies India's commitment to balancing the urgent need for data privacy with the goals of economic development and innovation. The legislation aims to create an ecosystem where technological advancement and individual rights can coexist.

However, the Act's ultimate success is not guaranteed. It will be determined by three key factors:

a. Effective Implementation: How the law is put into practice on the ground.

b. Consistent Enforcement: The real-world consequences for non-compliance.

c. Future-Proofing: Its ability to adapt to the rapidly evolving digital landscape.

By fostering a collaborative, transparent, and inclusive approach, India has the opportunity to set a global benchmark in digital governance. This will ensure that the benefits of technological progress are realized without compromising the fundamental rights of its citizens.

References

Books

1. Aditi Agarwal, Data Protection Laws in India: Privacy and Surveillance (Eastern Book Company, 2021).

2. Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs, 2019).

3. Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives (Oxford University Press, 2014).

4. Daniel J. Solove, Understanding Privacy (Harvard University Press, 2008).

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

6. Daniel J Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (Yale University Press 2006)..

7. BL Wadhera, *Law Relating to Intellectual Property* (5th edn., Universal Law Publishing 2011)..

8. Asha Kaushal, *Privacy and Data Protection: India and the EU* (Eastern Book Company 2023).

9. Raghavan Krishnan, *Data Privacy and Economic Development in India* (Oxford University Press 2021).

10. Nair Madhav, *Regulatory Challenges in India's Data Protection (Sage Publications 2022).*

11. Suresh Das, *Privacy vs. State Surveillance in India* (LexisNexis 2022).

12. Vikram Sharma, *Data Protection and Digital Literacy in India* (Thomson Reuters 2023).

13. Arjun Patel, *Data Governance and Emerging Technologies* (Cambridge University Press 2023).

14. Edward J Bloustein, *Individual and Group Privacy* (Routledge 2019).

15. Neeraj Sharma, *Data Localization and Sovereignty in India* (Oxford University Press 2022).

16. Anupam Chander, *The Electronic Silk Road: How the Web Binds the World Together in Commerce* (Yale University Press 2013).

17. Samir Saran, *The New World Order: Data Privacy and Protection in Emerging Economies* (HarperCollins 2023).

Articles and Journals

1. S. K. Verma, "Privacy, Big Data, and the Indian Legal Framework," Indian Journal of Law and Technology, vol. 16, no. 2, pp. 55–78, 2021.

2. Rolf H. Weber, "Transborder Data Flows: An International Privacy Challenge," Duke Law & Technology Review, vol. 14, no. 3, pp. 66–89, 2020.

3. Siddharth Tiwari, "An Analysis of GDPR and Its Implications for Indian Businesses," NALSAR Law Review, vol. 13, no. 1, pp. 45–67, 2019.

4. Krishnamurthy et al., "Cross-Border Data Transfers: A Legal Perspective," Journal of Data Protection & Privacy, vol. 4, no. 1, pp. 23–40, 2020.

5. Nehaa Chaudhari, "Regulating AI: The Indian Data Protection Perspective," Indian Law Review, vol. 2, no. 3, pp. 110–135, 2021.

6. Anupam Chander, "The Technological Sovereignty Debate in India," Georgetown Law Technology Review, vol. 3, no. 2, pp. 89–115, 2020.

7. Helen Nissenbaum, "Privacy as Contextual Integrity," Washington Law Review, vol. 79, pp. 101–139, 2004.

8. Chaudhary A, 'Comparative Analysis of Data Protection Laws: India vs. GDPR' (2022)

15(3) *Journal of Cyber Law* 275-312.

9. Gupta R, 'Empowering Consumers: The Role of Data Protection in the Digital Age' (2021) 10(2) *Privacy and Technology Review* 135-168.

10. Mehta A, 'India's Data Privacy Regime: Comparative Reflections on the GDPR' (2023) 7(4) *International Journal of Data Privacy* 456-492.

11. Singh V, 'The Role of Consent in Digital Privacy: A Critical Examination' (2022) 12(1) *Indian Law Review* 89-120.

12. Kumar P and Das S, 'Data Localization vs. Global Data Flow: Legal Challenges for India' (2023) 19(2) *Journal of International Law and Policy* 321-359.

13. Bose R, 'The Impact of Data Protection Laws on Innovation in India' (2023) 8(3) *Journal of Technology and Society* 192-225.

14. Jain S, 'Data Fiduciaries and Their Obligations Under the DPDP Act' (2022) 14(2) *Indian Journal of Cyber Law* 241-268.

15. Dasgupta M, 'Cross-Border Data Transfers: India's Approach vs. International Standards' (2023) 11(5) *International Data Privacy Journal* 567-605.

Reports

6. Dr. Justice B.N. Srikrishna, Report of the Committee of Experts on Data Protection Framework for India (MeitY, 2018).

7. Ministry of Electronics and Information Technology (MeitY), White Paper of the Committee of Experts on a Data Protection Framework for India (2017).

8. NITI Aayog, Responsible AI for All: A Framework for India (2021).

9. Privacy and Civil Liberties Oversight Board (PCLOB), Report on the Surveillance Program Operated Pursuant to Section 702 of FISA (2014).

10. International Association of Privacy Professionals (IAPP), Global Privacy Laws: 2023 Edition (2023).

11. Internet and Mobile Association of India (IAMAI), The Future of Digital India: Balancing Privacy and Growth (2020).

12. Ministry of Electronics and Information Technology (MeitY), *The Digital Personal Data Protection Bill 2023: Draft Explanatory Notes* (MeitY 2023) 15-60.

13. NASSCOM, *Data Protection and the Indian Economy: An Analysis of Compliance and Growth* (NASSCOM Report, 2023) 12-54.

14. Internet and Mobile Association of India (IAMAI), *India's Data Economy: Opportunities and Challenges* (IAMAI 2023) 32-75.

15. Data Security Council of India (DSCI), *India's Digital Privacy Landscape: Trends and Challenges* (DSCI Report, 2022) 22-65.

16. World Economic Forum (WEF), *Global Data Protection: Trends and Implications for Emerging Economies* (WEF 2022) 45-90.

Web Resources

1. Ministry of Electronics and Information Technology (MeitY), *Digital Personal Data Protection Act Overview* https://www.meity.gov.in/

2. Data Protection Board of India, *Enforcement Guidelines and Compliance Requirements* https://dpbi.gov.in/

3. European Data Protection Board, *Guidelines on Cross-Border Data Transfers* https://edpb.europa.eu/

4. Internet and Mobile Association of India (IAMAI), *Data Privacy in India: Challenges and Opportunities* https://www.iamai.in/

5. Data Security Council of India (DSCI), *Impact of the DPDP Act on India's Digital Economy* https://www.dsci.in/

6. Privacy International, *India's Data Privacy Landscape: Key Trends and Developments* https://privacyinternational.org/.

7. World Economic Forum (WEF), *Emerging Data Protection Regulations in Developing Economies* https://www.weforum.org/.

8. Harvard Law Review, *India's Data Protection Challenges in the Digital Age* https://harvardlawreview.org/

9. NASSCOM, *Data Privacy and Protection: Industry Perspectives on the DPDP Act* https://nasscom.in/

10. Brookings Institution, *India's Role in Shaping Global Data Governance* https://www.brookings.edu/

11. Council on Foreign Relations (CFR), *Data Localization and National Security in India* https://www.cfr.org/

12. The Centre for Internet and Society (CIS), *Critical Analysis of India's Digital Personal Data Protection Act* https://cis-india.org/

13. TechCrunch, *How India's Data Protection Law Will Affect Tech Companies* https://techcrunch.com/

14. Financial Times, *India's Privacy Law: The Road Ahead* https://www.ft.com/

15. Forbes India, *Data Privacy and Consumer Trust: The Role of the DPDP Act* https://www.forbesindia.com/

16. Oxford Internet Institute, *The Global Implications of India's Data Protection Law* https://www.oii.ox.ac.uk/

17. Economic Times, *India's New Data Protection Law: Opportunities and Risks* https://economictimes.indiatimes.com/

18. Bloomberg, *The Future of Data Privacy in India* https://www.bloomberg.com/