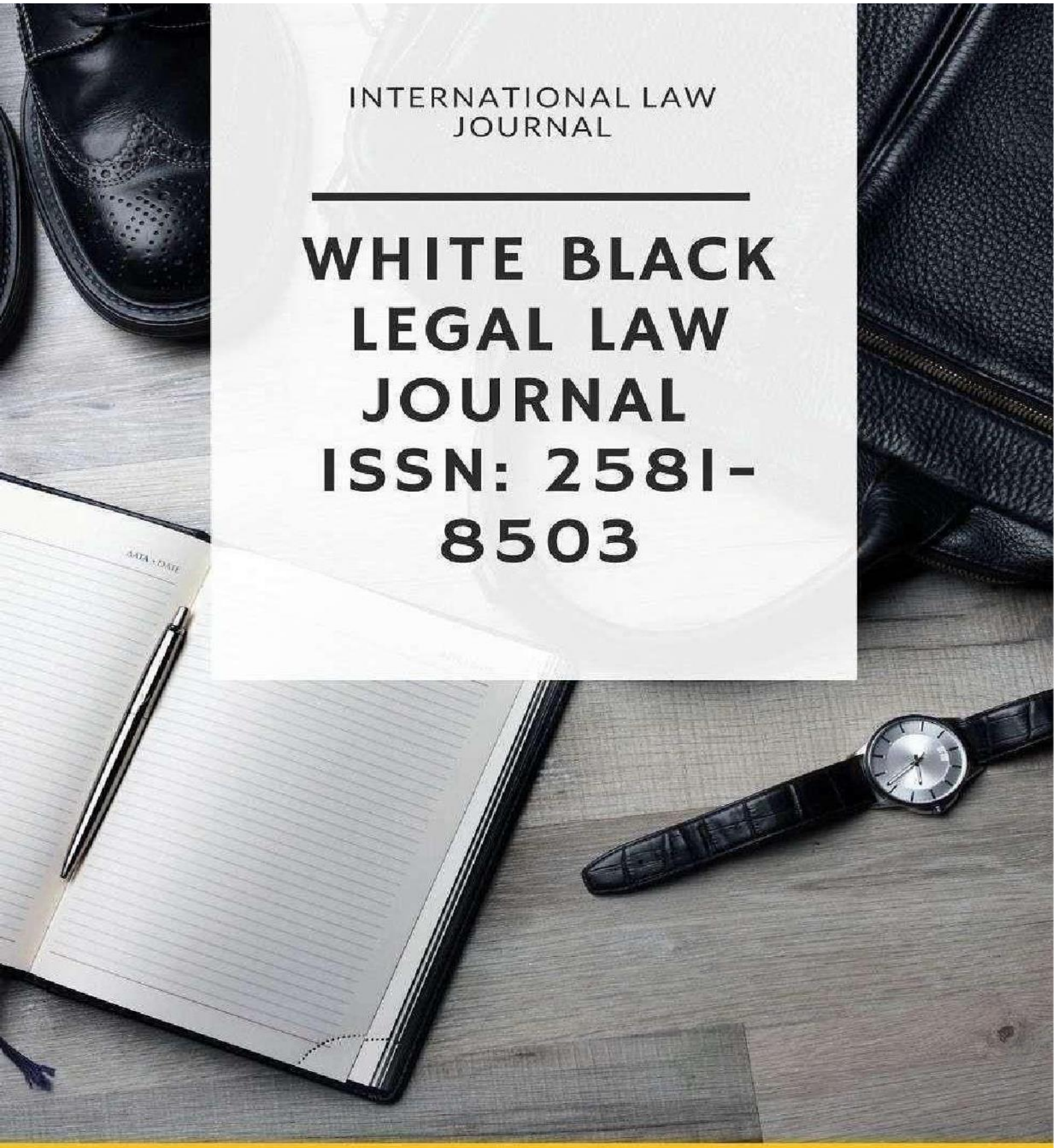

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 4 Issue 1 | Sep 2026 ISSN: 2581-8503

"FROM IT ACT TO DPDPA: TRANSFORMING INDIA'S LEGAL LANDSCAPE FOR DATA PROTECTION AND CYBERSECURITY"

AUTHORED BY - GURPREET SINGH[1] & DR ATUL KUMAR SAHUWALA[2]

INTRODUCTION

The digital revolution has revolutionized the way societies operate, introducing new opportunities for innovation, governance and commerce, and new risks for individuals of surveillance, cybercrime and misuse of information. India is one of the fastest growing digital economies with more than 800 million Internet users and is at the heart of this change. The Digital Personal Data Protection Act, 2023 (DPDPA) is a milestone in India's legislative history, as it is the first comprehensive law that seeks to safeguard personal data as per the principles of the Constitution and international best practices.

The IT Act, 2000 (IT Act) was a groundbreaking piece of legislation at the time, but it was not intended to cover the complexities of today's data processing environment, especially in the face of advancements in social media, artificial intelligence, and big data analytics.[3] In 2008, amendments were made to include concepts of data protection and intermediary liability but these were still sectoral and sketchy, lacking in a comprehensive system to protect informational privacy.[4]

In the light of judicial rulings putting privacy on the pedestal of a fundamental right, the inadequacy of the IT Act was coming to light. In K.S. Puttaswamy v. Union of India, the Supreme Court, in a nine-judge bench case, explicitly declared that the right to privacy is an inherent aspect of Article 21 of the Constitution and encompassed informational privacy, which was crucial for individual autonomy and dignity, and the potential misuse of personal information by the government and corporations, both of which threatened democratic governance. This precedent-setting decision gave the legislators a constitutional obligation to establish a strong data protection law.[5]

In response to this judicial order, in 2017, the Government of India formed the

[1] Research Scholar, Faculty of Law, Tantia University, Sri Ganganagar
[2] Assistant Professor, Faculty of Law, Tantia University, Sri Ganganagar
[3] Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
[4] Information Technology (Amendment) Act, No. 10 of 2009, INDIA CODE (2009).
[5] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

Justice B.N. Srikrishna Committee to draft a data protection law, which emphasized the importance of developing a rights-based approach to data protection that caters to privacy concerns while simultaneously fostering innovation.[6] A few drafts of the Personal Data Protection Bill were submitted from 2018 to 2021, but the bills were criticized for a lack of accountability and the extensive powers given to the government. Finally, Parliament passed the Digital Personal Data Protection Bill, 2023 which, after becoming law, is known as the DPDPA.[7]

The DPDPA brings into focus several important concepts which alter the way of doing business in India with regards to data governance. It identifies 'data fiduciaries' as those who decide on the purpose and means of the processing of personal data and 'data principals' as the individuals concerned by the processing.[8] Consent is set as the foundation of lawful processing with the requirement that consent must be given voluntarily, specifically and revocable by the person concerned. The Act also creates a Data Protection Board of India to handle disputes and enforcement. Significantly, the DPDPA provides individuals with rights to access, correct and remove their personal information.[9]

However, the Act comes with some controversy. This has drawn criticism from the critics, who claim that the DPDPA gives general exemption to the government, which means that they can bypass the consent and can process personal data for the sake of national security, public order, and other terms which seems vague.[10] Furthermore, there is no specific provision in the Act for the protection of "sensitive personal data," such as the European Union's General Data Protection Regulation (GDPR), which gives greater protection to health-related data, biometric data, and data on sexual orientation.[11]

The comparative perspective is key. Introduced in 2016, the GDPR is considered as the state of the art in data protection, in which accountability, transparency, and data minimization are key concepts and strict sanctions are provided in case of violations. In contrast, the enforcement mechanisms under the DPDPA seem to be less effective as the Data Protection Board is not fully independent and lacks adequate resources. This has raised the questions whether the framework is capable of being able to come up with the best practice in the world or whether it would become an Indian-style version, which sees state over individual

[6] Justice B.N. Srikrishna Committee Report, Ministry of Electronics & Information Technology (2018).
[7] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
[8] Id. § 2(11).
[9] Id. §§ 5–9.
[10] Id. § 17.
[11] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).

rights.[12]

At a cybersecurity level, the DPDPA is a step forward and has gaps. It requires data fiduciaries to take reasonable security measures, yet fails to encompass new threats, like ransomware, deepfakes, or Internet of Things (IoT) vulnerabilities.[13] The lack of any explicit mention of cross-border transfers or localization adds to India's complexity in global data flows. In India, businesses face risks of non-compliance, particularly in industries such as fintech, healthtech, and ecommerce, where personal information is a key component of their service offerings.

The constitutional aspects of the DPDPA are also crucial. The broadness or unrestricted use of government exemptions may render the Act susceptible to the proportionality test and ultimately the fundamental right to privacy may be infringed. Besides, the DPDPA intersects with other legislations like the IT Act, Bharatiya Sakshya Adhiniyam, 2023, and sectoral regulations by the Reserve Bank of India, which can create a complex legal landscape and potentially cause conflicts and ambiguities.[14]

Hence this research paper aims at critically analyzing the change from IT Act to DPDPA from a legal perspective. It will examine whether the DPDPA sufficiently resolves the cybersecurity and data protection issues in the digital era, its compatibility with Constitutional standards, and its compatibility with international standards. The study will also reveal the positive aspects of the Act, such as the recognition of individual right and the creation of a compliance mechanism, as well as the negative aspects, such as the over-intrusion of the government, and weak enforcement mechanisms. Finally, the paper will suggest that, although the DPDPA is a positive step, it needs significant change to ensure that India's digital future is secure and rights-respecting.

FROM IT ACT TO DPDP ACT

India's progress in the legal landscape of data protection and cyber security is indicative of the country's gradual acceptance of informational privacy as a constitutional and policy requirement. In the wake of the UNCITRAL Model Law on Electronic Commerce, the Information Technology Act, 2000 (IT Act) was India's first broad-based act to address electronic commerce, digital signatures and cyber offences.[15]

[12] Id. arts. 5–7.
[13] National Critical Information Infrastructure Protection Centre, Guidelines on Cybersecurity (2024).
[14] Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).
[15] UNCITRAL Model Law on Electronic Commerce, U.N. Doc. A/RES/51/162 (1996).

At the time, the IT Act was intended to facilitate e-commerce and give electronic contracts a legal leg to stand on. It criminalized such offences as hacking and unauthorized access to computers as well as tampering with computer source documents, but had a narrow definition of these activities – it did not anticipate the scale of data-processing, profiling, or surveillance which are inherent in the digital age.[16]

While Section 43A made a corporate liability provision to implement "reasonable security practices" on failure to protect sensitive personal data, the Rules gave no comprehensive rights-based approach to individuals.[17]

The shortcomings of the IT Act came to light through judicial interventions. The Supreme Court's decision in Shreya Singhal v Union of India against Section 66A of the IT Act, which prohibited offensive online speech, highlighted the need for a better equilibrium between state interests and individual rights in the IT Act.[18]

In the case of Justice K.S. Puttaswamy v. Union of India, the nine-judge bench held that informational privacy is a fundamental aspect of autonomy and dignity and that unchecked surveillance of personal information or misuse of it by corporations is a serious[19] threat to democracy. This resulted in a constitutional need for a strong data protection law.

The Government of India, on the other hand, has set up Justice B.N. Srikrishna Committee in 2017, which in its report A Free and Fair Digital Economy recommended a rights-based approach, an establishment of Data Protection Authority, and duties on the Data Fiduciaries. The Bill was introduced in 2019 and criticized for the lack of enforcement and excessive government exemptions and was withdrawn in 2022 for a new iteration.[20]

Meanwhile, further policy changes like the National Cyber Security Policy, 2013 and sectoral regulation from RBI and IRDA highlighted the increasing significance of cybersecurity, but these were still disjointed.[21]

In this context, the Digital Personal Data Protection Act, 2023 (DPDPA) was passed.[22] The DPDPA outlines the concepts of data fiduciaries (those who decide the purpose and means of processing) and data principals (individuals whose data is being processed). Consent as a basis for lawful processing is defined by clarity, informed choice, and

[16] IT Act, supra note 1, §§ 3–6, 65,66.
[17] Information Technology (Amendment) Act, No. 10 of 2009, INDIA CODE (2009).
[18] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
[19] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).
[20] Justice B.N. Srikrishna Committee Report, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians, Ministry of Electronics & Information Technology (2018).
[21] National Cyber Security Policy, Ministry of Communications & Information Technology (2013).
[22] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

revocability.[23]There are rights of access, correction and deletion for individuals, and security measures, notification of breaches and impact assessments put in place for fiduciaries.

Yet, controversies abound. This is a government exception for national security or public order, critics say, endangering privacy. The DPDPA does not define a separate class of "sensitive personal data," as the GDPR does.[24]

Comparatively, the GDPR is more oriented towards accountability, transparency and minimization, with independent supervisory authorities and robust penalties. The DPDPA's enforcement systems appear to be weaker with the Board lacking independence and resources; China's Personal Information Protection Law (PIPL) is a state-centric approach.[25]

There are limited cybersecurity implications. The Act does not provide for a comprehensive discussion on ransomware, deep fakes or IoT vulnerabilities and its provisions also do not explain the cross-border data transfers which add to India's challenge in the international arena of data.[26]

In the Constitution, the DPDPA will be examined for proportionality and necessity as enunciated in Modern Dental College v. State of Madhya Pradesh. The broad exemptions would pose a threat to privacy. There is complexity due to overlaps with IT Act, Bharatiya Sakshya Adhiniyam, 2023 and sectoral regulations.[27]

To summarize, India's shift from the IT Act to the DPDPA demonstrates the government's commitment to robust data protection measures. The IT Act provided a base, but wasn't sufficient. Judicial pronouncements, especially Puttaswamy gave rise to a constitutional obligation. While the DPDPA is a good development, there are concerns about its exemptions and enforcement. The success of India's digital future hinges on the ability of the DPDPA to become a comprehensive and rights-based framework that meets international standards.

[23] Id. § 2(11).
[24] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
[25] California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100–1798.199 (2018); Personal Information Protection Law of the People's Republic of China, Standing Committee of the National People's Congress (2021).
[26] California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100–1798.199 (2018); Personal Information Protection Law of the People's Republic of China, Standing Committee of the National People's Congress (2021).
[27] Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).

CRITICAL EVALUATION OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) is a landmark law in India's digital law landscape, which is the first comprehensive legislation aimed at the protection of personal data. However, the Act does give a clear definition of privacy rights and places duties on compliance while simultaneously having some serious structural flaws that have constitutional, institutional and policy implications. To do a critical evaluation of the DPDPA, it is important to look at the DPDPA in the backdrop of the constitutional jurisprudence as well as assessing the compatibility of DPDPA with international norms like General Data Protection Regulation (GDPR) of the European Union and its effectiveness so far in addressing the challenges of cybersecurity.[28]

The clear and most important aspect of the DPDPA is its recognition of privacy as a legal right and one which can be asserted in statutory ways. The DPDPA brings a change from the meager provisions of the Information Technology Act, 2000, which only put the onus on the corporations for failing to secure the personal data of their users and dealt only with corporations and their obligations, without giving any rights to those users. The DPDPA fills a constitutional vacuum by granting data principal rights to enforceable statutory provisions.

Another important development is the introduction of the Data Protection Board of India which can adjudicate the dispute and take remedial action, which is an improvement from the IT Act which did not have any institutional mechanism to enforce compliance.

The Act also places obligations on the data fiduciaries including reasonable security measures, notification of data breach, and data protection impact assessment in some instances, which mirrors the international practices and an awareness of the danger that can be created by large-scale data processing. The DPDPA aims at encouraging a culture of compliance within businesses and government bodies.

However, the Act is flawed in structure and so fails to achieve the desired effect, in spite of its strengths. It is Section 17 of the Act, which provides blanket exemptions for any of the government's agencies on the grounds of national security, public order or for any other reason, which is most problematic because it gives too much discretion to the Executive and raises concerns about excessive surveillance and loss of privacy rights. Without judicial or parliamentary control over these exemptions, the abuse of such exemptions is likely to be

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), arts. 51–59.

worse. The provision is also found to be unconstitutional on the ground that it does not meet the test of necessity, proportionality and adequate safeguards outlined in Modern Dental College v. State of Madhya Pradesh.[29]

Another limitation is the enforcement scheme. The Data Protection Board is far from independent and not insulated from judicial interference and its composition and appointment continues to be subject to government control. This institutional solution weakens the effectiveness of the mechanism and potentially makes the Board just a compliance facilitator instead of a rights-protecting institution.

The DPDPA does not recognise the idea of "sensitive personal data" as it is done in the GDPR, and thereby the protection of sensitive categories of data is lessened, especially in sectors like health, finance and biometric identification. It is curious that the government did not include biometric data in the lists of the initiatives it plans to implement because India has already had concerns about biometric information in various programmes, including Aadhaar.

Comparing the two, the DPDPA aligns with GDPR on topics like transparency, consent and rights of individuals, but falls short on the accountability of the state and the independence of enforcement. India's DPDPA thus falls somewhere between the two but it seems to be more state-centric, with government control over the Board of Directors, imposing lower penalties, and having broader opt-out rights under the CCPA.

The lack of cybersecurity aspects further reveals the shortcomings of the Act. The DPDPA does not provide a holistic coverage of new vulnerabilities like deepfakes, ransomware or vulnerabilities of Internet of Things (IoT) devices, which makes India's situation more complex in international data transfers.[30] The uncertainty over compliance is a major challenge for businesses in India, especially in sectors such as fintech, healthtech, and e-commerce, where personal information plays a crucial role in their operations. Lack of localization requirements or adequacy standards for foreign jurisdictions leads to regulatory ambiguity and can impede international cooperation.

From a constitutional perspective, the DPDPA needs to go through proportionality and necessity tests. The Supreme Court in Puttaswamy made it clear that the right to privacy must be limited in a very specific manner, and must be guarded by safeguards; Section 17 also has sweeping exemptions which could prove unconstitutional. Furthermore,

[29] Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).
[30] National Critical Information Infrastructure Protection Centre, Guidelines on Cybersecurity (2024).

there is a complex legal system that is likely to cause conflicts and ambiguities, as there is an overlap between the DPDPA and other laws, such as the IT Act, the Bharatiya Sakshya Adhiniyam, 2023, and sectoral regulatory requirements issued by the Reserve Bank of India.

It's also important to think about the challenges to the implementation in a critical evaluation. Institutional capacity, technical knowledge and public awareness are still limited in India and they are crucial for enforcement. The effectiveness of the Data Protection Board will depend on attracting and enlisting good personnel and establishing technical infrastructure. The absence of resources also puts the Board at risk of becoming a symbol of a regulator without any resources. Few people are aware of their privacy rights, especially in rural areas, and access to remedies is an issue.

Suggestions for reform involve limiting government exemptions to meet the requirement of proportionality, increase the independence of the Data Protection Board, establish a category of sensitive personal data with increased protections, improve the institutional capacity, and harmonize the DPDPA with sectoral laws and international instruments. The ratification of international conventions like the Budapest Convention on Cybercrime may also help India to cooperate better with other countries in the world.[31]

Overall, the DPDPA marks a significant advancement in India's digital privacy landscape, outlining privacy rights and compliance guidelines. However, flaws such as government exemptions, inadequate enforcement, and the absence of sensitive data classification are significant concerns. In order to establish a privacy respectful digital environment in India, the Act should be modified so that it reflects constitutional values and international standards, while being responsive to the challenges of cybersecurity. The shift from IT Act to DPDPA highlights the complex nature of finding a balance between innovation, security, and fundamental rights in the digital era. The evolution of the DPDPA into a comprehensive and rights-centric framework that balances privacy rights with technological advancement will shape India's trajectory towards a digital economy.

Conclusion

The journey from the initial efforts in data protection law to the enactment of the Digital Personal Data Protection Act, 2023, is a significant milestone and a challenge in India's digital governance journey. India has seen the evolution of technology, judicial decisions, and international influences since the inception of the Information Technology Act,

[31] Budapest Convention on Cybercrime, Council of Europe Treaty No. 185 (2001).

2000, which mainly aimed to legalize electronic commerce and tackle elementary cyber offences, through the introduction of the Fundamental Right of privacy in the Puttaswamy case. This historical evolution culminated in the DPDPA, which promises to be a rights-centric approach to privacy protection and demonstrates the conflicting interests between privacy, government authority, and economy development.

The essence of the DPDPA is that India recognizes that personal information is not just a business asset but a part of human dignity and autonomy. The Act seeks to give people more power, by providing a framework for rights like access, correction, and erasure, and by making consent the fundamental principle of lawful processing in a world where data is the currency of digital interactions. This is a dramatic shift from the narrow definition of IT Act, which places emphasis on corporate liability and technical compliance. It mirrors a developmental process of the constitution, moving towards convergence with the Supreme Court's formulation of privacy as a right to respect for life and liberty, as an inherent right.

The Data Protection Board of India is a testament to the legislature's commitment to set up institutional structures to ensure enforcement. India now has a specific organisation to resolve conflicts, levy fines and create compliance with data protection standards. This institutional innovation holds importance because it breaks the silos of the past that saw the regulation of different aspects of the industry in different agencies like the Reserve Bank of India or the Insurance Regulatory and Development Authority. Overall, the Board represents a unification of authority and power in data protection matters, providing a consistency and accountability.

However, the DPDPA's strength is somewhat marred by its structural flaws, which pose substantial doubts as to the effectiveness of the law. What's worst is the extent of the government exemptions! The Act could be used by the executive to excuse its agencies from compliance, for reasons of national security or public order, and therefore allows for the normalization of surveillance and the undermining of the very rights which it aims to protect. However, such broad discretion is counter to the concepts of proportionality and necessity in a constitutional democracy, where privacy is recognized as a fundamental right. The lack of judicial or parliamentary control over these exemptions exacerbates the situation, and allows executive power to run wild.

No less awkward is the enforcement structure. The establishment of the Data Protection Board is laudable, but it is unclear whether it will be independent. The composition and appointment of the Board are subject to government control and it is not clear that it can act impartially against state agencies. An independent Board is crucial to ensuring the Board's

role is one of rights protection instead of compliance facilitation. This institutional structure weakens the credibility of the enforcement mechanism and reduces citizens' confidence in the system.

The DPDPA also does not make any distinction between sensitive personal information and normal personal information. While the GDPR provides additional safeguards for data categories like health, biometrics, sexual orientation etc., the Indian regulation addresses personal data in a similar manner for all categories. This is especially alarming because in a country where biometric information is heavily relied upon in various programmes like Aadhaar and where health and financial information is increasingly digitized. Sensitive data are not adequately protected, reducing the protection purpose of the law.

The DPDPA is, from a comparative perspective, convergent and divergent with global standards. It overlaps with GDPR in points like consent, accountability, individual rights, but has significant differences in accountability of the states and independence of enforcement. The GDPR's powers for independent supervisory authorities and heavy fines are significantly different from the DPDPA with its government controlled Board and limited penalties. Likewise, the California Consumer Privacy Act focuses on consumer rights and transparency, while China's Personal Information Protection Law is more state-oriented, India's DPDPA falls somewhere in between, but tips the scales towards executive powers. The position puts India in a dilemma regarding its capability to uphold the sanctity of privacy in practice, and retain trust in data governance at the international level.

Further, gaps are revealed in the Act in the context of cybersecurity implications. The DPDPA does not provide any specific protection for new threats like ransomware, deepfakes, vulnerabilities in IoT devices, etc. Nor does it give clarity in cross border data transfer, which taints India's position in cross-border data flows. Foreign jurisdictions, however, have no clear requirements that they must meet to be deemed ‘adequate' or that a ‘localisation requirement' applies to them, meaning there is regulatory ambiguity in an era where data is transnational and cyber threats are borderless. In today's India, concerns about uncertainty are not limited to sectors like fintech, healthtech and e-commerce where personal data is essential for service delivery.

The principles expressed in Puttaswamy and subsequent cases need to be the yardstick for constitutionally evaluating the DPDPA. Restrictions on privacy must be clearly specified, be necessary and have protections. This is not true for the large exemptions granted in Section 17, which could be unconstitutional. Furthermore, the compatibility of the DPDPA with other laws, like the IT Act and Bharatiya Sakshya Adhiniyam, can cause conflicts and

confusion. The need of the hour is the need for harmonization of these frameworks to prevent regulatory fragmentation and provide coherence in the digital governance framework in India.

Implementing it complicates the picture even more. Enforcement relies on institutional capacity, technical expertise and awareness which are still lacking in India. The success of the Data Protection Board will depend on the quality of the people that can be recruited and technical infrastructure development. The Board's effectiveness in regulating is threatened to be a hollow shell, if the Board does not have the necessary resources. Limited awareness of privacy rights, especially in rural areas, also exists, compounding concerns of remedy availability.

The DPDPA, as such, is both a step forward and a danger. It sets out privacy rights, compliance framework and also brings India to the current world trends. However, its limitations – exemptions by the government, weak enforcement, insufficient categorization of sensitive data and implementation problems – pose significant concerns. The Act needs to be evolved to create a privacy-conscious digital ecosystem for India. To that end, the reforms should comprise of reducing the scope of government exemptions, improving the independence of the Data Protection Board, creating a new category for sensitive personal data, increasing institutional capacity, and harmonize the DPDPA with the sectoral regulations and international frameworks. India’s cooperation on international issues may also improve with the ratification of international conventions like the Budapest Convention on Cybercrime.

Overall, the shift from IT Act to DPDPA highlights the complexities of striking a balance between innovation, security, and fundamental rights in the digital age. The IT Act provided the basis for regulating electronic commerce and cyber offences but the Act was found to be insufficient to deal with the complexities of modern data processing. The recognition of privacy as a fundamental right in the case of Puttaswamy also put an obligation on the judicial system to reform. While the DPDPA is a positive development, there are concerns about its effectiveness due to its shortcomings.

Whether the DPDPA will evolve into a comprehensive and rights-oriented framework that safeguards the rights of individuals while fostering technological advancement will shape India's digital future. The consequences are serious: In a country with more than 800 million internet users, where financial transactions, healthcare or other matters are carried out via digital platforms, the protection of personal data is not only a legal matter but also a matter of society. The DPDPA needs to address this challenge and ensure that the Indian digital transformation is built on the values enshrined in the Constitution, the best practices in the world and the dignity of the individual.

Finally, the DPDPA is a milestone and a mirror. It is a sign of India's desire for a more private digital environment, and a display of the conflict between state authority and personal freedoms. While the law is a step towards a new era of digital governance in India, its impact will rely on the resolve and commitment of policymakers, regulators, and the public to address its shortcomings and continue the path of reform. This is the dynamic between technology, law and constitutionalism best reflected in the journey from the IT Act to the DPDPA. The years to come will prove to test India's ability to strike a balance between innovation and rights, security and liberty, and economic growth and human dignity. All these hurdles have to be overcome to make the DPDPA a game-changer in India's data protection and cybersecurity framework.