A CONSTITUTIONAL PERSPECTIVE ON PRIVACY RIGHTS AND DATA PROTECTION LAWS IN INDIA

Sharfaraj Husain

INTRODUCTION

In the information age where we use digital tools for almost everything in our daily activities, little do we know about us creating eternal digital foot Prints. As we live of our lives on the Internet, we are creating a permanent record of unparalleled pervasiveness and depth. Indeed, almost everything on the Internet is being archived. Our online identities are reflected in our websites and social media posts. However, almost little is lost or forgotten when we delete or update material on the Internet. The quantity of information stored will only increase as our lives become continually digitized into the domain of cyberspace.

The issue of data protection and privacy is not limited to one country. While regional laws like the GDPR are important, global privacy standards are mostly shaped by international guidelines such as the Organization for Economic Co-operation and Development (OECD) guidelines, the UN principles, the Asia- Pacific Economic Cooperation (APEC) framework and convention 108+. Ensuring a free flow of transborder data and, to a considerable part, allowing for the protection of people' private lives by limiting governmental intrusion are the goals of these international data protection frameworks. The Personal Data Protection Act of 2023 [1]in India was heavily influenced by the applicability of data protection laws from other countries. The establishment of data protection regulations in India is a direct result of the growing international concern about the security of personal information.

CONSTITUTIONAL ASSEMBLY DEBATE ON RECOGNITION OF RIGHT TO PRIVACY

The Constituent Assembly debated the provisions of Constitution of India for 166 days over a

[1] Digital Personal Data Protection Act 2023 (No 22 of 2023) Gazette of India, 11 August 2023

span of nearly two years[2]. During the debates, Mr. B.N. Rau (Adviser to the constituent Assembly) and Alladi Krishnaswamy Ayyar both opposed the inclusion of the right to privacy within the fundamental rights framework. BN Rau expressed concerns that right to privacy could hinder police investigative powers and disrupt the investigation process[3]. Meanwhile, Ayyar argued that recognizing the right to privacy and correspondence secrecy would have detrimental effects on civil litigation, where documents play crucial role as evidence[4].

Throughout the plenary sessions of the Constituent Assembly, there were two separate efforts to incorporate provisions related to the right to privacy into the fundamental rights[5].

Somnath Lahiri proposed making the right to correspondence privacy a fundamental right on April 30, 1947. His suggestion, though was not well received. A year later, Kazi Syed Karimuddin made a motion to amend Article 20 (Draft 14) of the constitution to protect people's right to be free from arbitrary searches and seizures of their person, home, papers and belongings. Both of these attempts to include right to privacy as a fundamental Constitutional right failed[6].

On the one hand, a careful analysis of the debates shows that the Assembly focused only on whether to explicitly include a provision guaranteeing the right to privacy, and that too, specifically in the limited context of "searches" and "secrecy" of correspondence. On the other hand, it is noteworthy that the broader aspect of the right to privacy were not thoroughly explored. The question of whether the term "liberty" under article 21 also covered various elements of the right to privacy was not addressed during the discussions.

This does not imply that the Constituent Assembly officially resolved to reject mention of the right to privacy as an essential component of the liberty and freedoms protected by the fundamental rights. Since the Assembly rejected the inclusion of the right to privacy, no

[2] "The constituent assembly sat for the first time on 9th December 1946. Over the next 2 year and 11 months, the assembly sat for a total of 166 days to frame the Indian constitution, the final session of the constituent assembly took place on the 24th January 1950."

[3] Constituent Assembly Debates, vol VII (6 December 1948) 931 https://cadindia.clpr.org.in/constitution_assembly_debates/volume/7/1948-12-06 accessed 25 July 2025.

[4] R Krutika, 'The right to privacy in Indian constitutional History' (constitution of India, 20 August 2020) https://www.constittutionofindia.net/blogs/the_right_to_privacy_in_indian_constitutional_history accessed 21 may 2025.

[5] Dr. Sunil Khosla, 'The right to privacy: constitutional perspective in India' (2017) Innovative Research thoughts 121-127 https;//irt.shodjsagar.com/index/php/j/article/view/526 accessed 21 may 2025.

[6] Constituent Assembly Debates, vol 7, 2 December 1948, 806-07

separate provision for it is made in the Constitution under part III. The recognition of the right to privacy within the Indian Constitutional framework has evolved gradually, beginning with the debates of the Constituent Assembly and later taking shape through judicial interpretation and Constitutional provisions.

The constitutional foundation reflects a broader understanding of dignity and individual worth in society. In this regard, Ronald Dworkin believes that the government should treat everyone equally with care and respect[7]. Individuals have inherent dignity and moral worth, independent of who they are or where they stand, which the state must not simply recognize passively, but actively care about. The state constitution should provide basic human rights to citizens, allowing them to live decent lives.[8]

The Preamble of the Indian Constitution sets out the nation's fundamental values- Justice, Liberty, equality and Fraternity- all of which aim to ensure the dignity of the individual. This dignity is closely linked with the right to privacy. Liberty of thought, expression, belief, faith and worship as promised in the preamble, includes the freedom to form personal choices without fear or interference. Such freedom naturally requires a private space – both physical and mental. Privacy allows individuals to shape their identity, maintain personal relationships and protect their autonomy. Therefore, the values in the preamble, especially liberty and dignity form the moral foundation for recognizing the right to privacy in India.

While the Constitution ensures justice and equality for all, these values also form the moral base for the protection of privacy. Article 14 which guarantees equality before the law, supports the idea that every individual has an equal right to enjoy personal autonomy and private space without arbitrary interference. The dignity of a person protected through equality cannot be truly realized unless individuals are allowed to make personal choices regarding their body, home, thoughts and information. Thus, equality and dignity together form a strong foundation for recognizing the right to privacy under the Indian Constitution.

Natural Justice values, such as justice, equity, and fairness, are recognized in Article 14 of the Indian Constitution. When human rights and fundamental freedoms are infringed, Article 14's justice principles come in and restrict all government acts. In fact, the judiciary frequently these

[7] Ronald Dwarkin, Justice for Hedgehogs (Harvard University Press, 2011) 55-57
[8] Rhoda E Howard and Jack Donnelly, 'Human Dignity, Human Rights, and political Regimes' (1986) 80 (3) American Political Science Review 801, 803.

concepts in evaluating arbitrary and discretionary powers. The Indian SC has ruled that administrative entities must always act in accordance with the "Fairness" principle. The parliament cannot overlook the principles of natural justice when passing any legislation. Articles 14, 19 and 21 together support the idea that people's rights cannot be taken away by the government. If it does, they will have to implement a fair, reasonable and just process. Lesbian and gay rights have recently been acknowledge on the basis of Article 14. The government's irrational and irrational choice to restrict the rights of gays and lesbians is an infringement on their right to privacy[9].

In general, 'freedom and speech and expression' is seen as the polar opposite of 'right to privacy'. However, freedom of speech and expression includes the right to talk freely and anonymously, which is a part of the "right to privacy"[10]. Although the Constitutional structure allows parliament to legislate on matters related to Data Protection under Article 246(1) read with List I of the Seventh Schedule, the content of such laws must still pass the test of fundamental rights.

Since the right to privacy has been firmly placed under Article 21 by the SC in the Puttaswamy Judgment, any law that limits or interferes with privacy must satisfy the requirements of legality, necessity and proportionality. The real test is not only whether parliament holds authority to make law, but whether that law respects the dignity, autonomy and personal liberty guaranteed by Article 21. Thus, the right to privacy is not a secondary concern but the Constitutional standard against which all data protection laws must be measured.

REGULATORY FRAMEWORK OF DATA PROTECTION IN INDIA

India's legal framework for Data Protection involves both civil and criminal aspects. When someone unlawfully accesses or misuses another person's data, it is treated as a privacy violation and can lead to both civil and criminal penalties. Efforts to safeguard privacy began in 2000 through the Information Technology Act, which, for the first time, included digital data within the scope of protection. In 2006, the government put forward a draft Personal Data Protection Bill aimed at establishing legal safeguards for personal information. Later, in 2011, a draft Right to Privacy Bill was also introduced to address increasing issues associated with

[9] Naz Foundation v Government of NCT of Delhi 2010 cri LJ 94 (Del HC).
[10] Daniel J Solove, The Digital Person: Technology and Privacy in the information age (NYU Press 2004) 26.

the protection of individuals' private data.[11]

INFORMATION AND TECHNOLOGY ACT, 2000

In India, the IT Act of 2000 represents the inaugural legislation focused on information technology, addressing issues related to e-commerce, e-governance and cyber-crimes. Additionally, it serves as the legal framework for data protection. The primary objective of the It Act is to safeguard against the violation of information caused by data breaches from computers. It includes several provisions, such as section 65 and section 66 which prohibit unauthorized use of technology including computers, laptops and the information stored on them.

I. Section 43 of the IT Act stipulates penalties for the destruction of data stored on computers. According to this section, if an individual utilizes computer data without authorization or engages in illegal activities, they may face a penalty of up to 3 years in prison, a fine of 5 lakhs rupees, or both.

II. Section 65 deals with individuals who either knowingly or accidentally modify, destroy or hide any computer source code.

III. According to section 66, anyone who damages or modifies data saved on a computer will be held accountable for the offense. Three years in prison, a fine of two lakh rupees, or both are the penalties stipulated in these sections.

IV. Additionally, if a company breaches the provisions of the IT Act then the managers of the company and directors are in person liable for the offense.

The Information Technology (Amendment) Act, 2008 was enacted to address the gaps left by the original Act and to strengthen the legal framework relating to information technology and digital security. Among other changes, the Amendment introduced Section 69A, which empowers the Central Government to order the restrictions of public access to certain information through computer resources and also to intercept, monitor or decrypt information in the interest of national security. However, this provision drew widespread criticism due to

[11] Right to Privacy Bill 2011 9Department of Personnel and Training, Government of India https://www.prsindia.org/uploads/media/draft/draft%20right%20to%20privacy%20bill,%202011.pdf accessed 25 July 2025.

concerns over excessive government control. In Shreya Singhal v UOI[12], the SC in 2015 upheld the Constitutional validity of section 69A, noting that the section incudes adequate procedural safeguards to prevent misuse.[13]

THE INDIAN TELEGRAPH ACT, 1885

As per section 5(2) of the Indian Telegraph Act, the government holds the power to intercept messages, but only under the conditions laid out in the law. Because such interception involves accessing private conversations, it directly affects an individual's right to privacy and

must be used cautiously and lawfully. This power can be exercised only when there is a public emergency or a threat to public safety. Without the presence of either, the authority has no right to carry out such interception.

The SC addressed this issue in the landmark ruling of People's Union for civil liberties v. Union of India[14]. The court clarified that the power under section 5(2) cannot be used unless a real public emergency exists or public safety is genuinely at risk. It also stressed the importance of proper procedural checks to ensure that surveillance powers are not abused and that individual privacy, as guaranteed in Article 21 of the Constitution is respected.

THE DIGITAL PERSONAL DATA PROTECTION ACT,2023

India's journey towards data privacy protection has been gradual one, evolving from fragmented regulations to the current comprehensive framework. Before the rise of information technology, there were minimum legal safeguards for data protection in India. Privacy rights were mostly protected under common law principles. Unfortunately, there was no specific data protection laws existed.

In 2017, the SC recognized right to privacy as a fundamental right guaranteed under Article 21 of the Indian Constitution, laying the foundation for a structured Data Protection regime in India. Following this, the Government of India set up a committee chaired by Justice B.N. Srikrishna to draft a Data Protection framework. The committee submitted its report in 2018,

[12] Shreya Singhal v UOI [2015] AIR SC 1523
[13] Indian Express, 'SC strikes down section 66 of IT Act, upholds validity of section 69A' (24 March 2015) https://indianexpress.com/article/india/india-others/sc-strikes-down-section-66a-of-it-act-upholds-validityofsection-69a/ accessed 25 July 2025.
[14] People's Union for civil liberties v. Union of India AIR 1997 SC 568.

highlighting the urgent need for a law to safeguard personal data in the digital age. Among its key recommendations were: recognizing privacy as a core value, enforcing data minimization, ensuring informed consent, establishing a Data Protection Authority (DPA) and creating obligations for both government and private entities handling data.

The 2018 report by the Justice B.N. Srikrishna Committee laid the foundation for shaping India's data privacy framework[15]. The committee was formed in response to rising concerns around data misuse and privacy violations after the SC's declaration of privacy as a fundamental right in the Puttaswamy Judgment. The report recommended the creation of a strong and independent law to protect personal data and introduced key principles like data minimization, purpose limitation, user consent and accountability of data fiduciaries.

Following this, the Personal Data Protection Bill (PDP Bill) was drafted and introduced in 2019.it underwent multiple revisions, public consultation and industry feedback over the years. Finally, after nearly a decade of deliberation, the Digital Personal Data Protection Bill, 2023 was tabled in the monsoon session of parliament. It was approved by the Lok Sabha on August 7, 2023 and by the Rajya Sabha on August 9, 2023. The bill received presidential assent on August 11, 2023 and officially became the Digital Personal Data Protection Act, 2023. However, the Act has not yet come into force, as the government is still expected to issue a formal notification for its implementation.

The act aims to strike a balance between protecting individuals' personal data and permitting its use for legitimate purposes such as innovation and economic growth while keeping user consent and accountability at its core. The DPDP Act covers the handling of digital personal data within India in two scenarios; firstly, when such data is obtained in digital format from data principles; and secondly when such data is initially gathered in non- digital form and then digitized. As a result, the DPDP Act does not apply to non-digitized personal data processing. Furthermore, the scope of the statute has been broadened.

It has an extraterritorial applicability, which includes the processing of digital personal data outside of India's boundaries if it relates to the provision of goods or services to data principals in India.[16] Notably, the DPDP Act does not specifically state whether its provisions apply to the

[15] Justice BN Srikrishna Committee Submits Data protection Report (Drishti IAS, 27 july 2018) https://www.drishtiias.com/daily-news-analysis/justice-bn-srikrishna-committee-submits-data-protectionreport
[16] Digital Personal Data Protection Act 2023, s 3(b)

processing of personal data belonging to data principals located outside of India. It grants certain exceptions to the startup from the stringent provisions. The term "Personal Data" has been introduced in the Act.[17]It imposes an obligation on data fiduciaries to secure personal data in their custody by implementing reasonable security measures to avoid breaches. The data fiduciary is required to notify both the board and the impacted data principles in the case of a data breach. The method of notification, however, is left to be determined. When it comes to the handling of personal data, the act clearly defines it to include collection, recording, organization, storage, adoption, retrieval, utilization, alignment, combination, indexing, sharing and disclosure of personal data. With regards to the handling of personal data of child, the act mandate to obtain the consent of the parent[18]. The notion of a 'Data Principal' has been significantly broadened.[19]

It now not only covers individuals but also encompasses parents or legal guardians of children whose personal data is in question. Furthermore, the definition has been expanded to include legal guardians of "individuals with disabilities"[20].The Act deals with data fiduciary as well. According to the DPDP Act, a data fiduciary is anyone, whether individually or in collaboration with others, who determines the objectives and methods for processing personal data. Data fiduciaries are permitted to handle personal data only for lawful purposes, subject to obtaining consent. This consent needs to meet certain criteria: it must be freely given, specific, informed, unconditional and unambiguous. It requires an explicit affirmative action from the data principal to indicate their agreement to the handling their personal data for the specified and necessary purpose.[21] The request must be presented in a plain and straightforward manner, take away the option to agree to the request in either English or any of the 22 languages listed in the eighth schedule to the Indian Constitution[22]. The request must include contact information for the data protection officer or an authorized representative who can handle communications from the data principal.

[17] Digital Personal Data Protection Act 2023, s 2(t)
[18] Digital Personal Data protection Act 2023, s 9
[19] Digital personal Data Protection Act 2023, s 2 (j)
[20] Digital Personal Data Protection Act 2023, s 9
[21] Supratim Chakraborty and Himeli Chatterjee, 'India's Digital Personal Data Protection Act, 2023: Impact on Hospitality Sector' (SCC Online Blog, 12 August 2023 https://www.scconline,com/blog/post/2023/08/22/indiasdigital-personal-data-protection-act-2023-impact-onhospitality-sector/ accessed 26 may 2025.
[22] AZB & Partners, 'Digital Personal Data Protection Bill, 2023- key Highlights' https://www.azbpartners.com/bank/digital-personal-data-protection-bill-2023-key-highlights accessed 26 may 2025.

Additionally, a data fiduciary must provide a comprehensive notice to the data principal either during or before seeking consent. This notice should cover several important elements, firstly, explanation of personal data to be collected and the aim behind it will be processed. Secondly, description of the data principal's rights, including the right to correction, withdrawal of consent, and the procedure for filing complaints with the board. Thirdly, clarity on how a complaint can be lodges with the board. In cases where consent was granted before the enactment of the DPDP Act, the data fiduciary must provide such notice "as soon as it is reasonably practicable".

This notice should be presented in plain language either as a separate document, electronically, or in a manner as specified by regulations.[23] Under the DPDP Act, certain violations, including the failure to prevent personal data breaches, can result in penalties of up to INR 250 Crore. Importantly, the previous cap of INR 500 Crore for single-instance penalties has been eliminated[24]. Unlike earlier versions, this law does not allow data principals affected by breaches to seek compensation from data fiduciaries. Instead, the board can now impose penalties of up to INR 10,000 on data principles who fail to fulfill their obligations.

GAPS AND AMBIGUITIES IN INDIA'S DATA PROTECTION ACT

Despite being a landmark step towards recognizing the right to privacy in the digital age, the Digital Personal Data Protection Act, 2023 is not without its flaws. While it lays down a broad framework for data governance, or silent on key aspects. These gaps raise significant concerns regarding accountability, enforcement and the actual protection of individual rights. A closer look at these shortcomings reveals that the Act may fall short of ensuring a truly robust and rights-based data protection regime.

1- VAGUE PROVISIONS AND LACK OF CLARITY

Several digital rights organizations and legal experts, such as the Internet Freedom Foundation (IFF) and the Internet Society, have raised concerns about vague provisions in the Draft Digital Personal Data Protection Rules, 2025. For example, Rule 6 requires data fiduciaries to implement 'reasonable security safeguards" under Section 7(b), but does not define what is considered "reasonbale", which may lead to inconsistent compliance and

[23] Digital Personal Data Protection Act, s 6
[24] Digital Personal Data Protection Act 2023, Schedule 1

enforcement. Similarly, Rule 5 gives the government broad powers to process personal data for purpose like granting benefits or license, but lacks sufficient safeguards or limitations, raising fears of potential misuse. Moreover, experts have criticized the opaque consultation process. IFF pointed out that public comments were treated confidentiality, weakening transparency and public engagement. Another concern is Rule 10, which requires parental consent for processing a child's data. Experts note that this may require linking children's data to government IDs, increasing the risk of surveillance and excluding children whose parents lack digital literacy or documentation. These ambiguities in the draft rules could hinder effective implementation of the Act, increase compliance uncertainty for business and negatively impact individuals' privacy rights.

2- EXCESSIVE GOVERNMENT ACCESS TO DATA

The draft rules grant the government broad authority to access personal data under loosely defined circumstances, such as for "fulfilling a specific task in the public interest."[25] This expansive access raises concerns about potential overreach and misuse of personal information, undermining the very objective of data protection.

3- POTENTIAL FOR MASS SURVEILLENCE

Provisions related to age verification and data collection [26]could inadvertently lead to mass surveillance. By linking government-issued IDs to online credentials, there is a chance of creating extensive databases that monitor individuals' online activities, posing significant privacy concerns.

4- DATA MINIMIZATION AND RETENTION CONCERNS

The draft rules appear to overlook principles of data minimization and storage limitations. Data minimization means that only the personal data strictly necessary for a specific purpose should be collected, while retention limitation requires that such data should not be stored longer than necessary. However, the absence of clear guidance on these principles in the draft rules could lead data fiduciaries to collect excessive personal data or retain it indefinitely. This increase the chance of data breaches, unauthorized access and misuse of

[25] Digital Personal Data Protection Act 2023, s 36
[26] Digital Personal Data Protection Rules 2025, rule 10

personal information thereby weakening the individual's right to privacy and violating internationally recognized data protection norms.

5- LACK OF INDEPENDENT OVERSIGHT

The absence of an independent regulatory body to oversee data protection practices under the Digital Personal Data Protection Act 2023 is a significant shortcoming[27]. Without impartial supervision, there is a heightened risk of arbitrary decision- making, politicised enforcement and limited accountability in the handling of personal data. This not only undermines public trust but also weakens the individual's privacy rights as there is no neutral authority to ensure that government and private entities comply with data protection norms.

CONCLUSION

The Digital Personal Data protection Act 2023 represent a pivotal moment in India's data privacy landscape. These rules are set to reshape how organizations manage personal data, placing stronger emphasis on accountability, transparency and user rights. Businesses will be expected to adopt more structured data governance practices, ensure secure processing and comply with principles like data minimization and purpose limitation. Additionally, they must empower individuals with greater control over their personal information, including rights to access, correction, and erasure. While adapting to these new requirements may be challenging, they present an opportunity for companies to strengthen consumer trust and show a commitment to responsible handling of personal data. In a world where digital trust is becoming increasingly important, early and effective compliance will serve as a competitive advantage. In the digital age, government access to personal data has grown to be serious concern with important implications for privacy, civil liberties and individual rights. The DPDPA 2023 represents a significant advancement in addressing these issues. However, there are several issues and points of controversy with this law. The Act's data localization regulations offer an innovative method to securing information, especially for essential personal data. However, there are still concerns over the possible effects on international data flows and data security.

[27] Digital Personal Data Protection Act 2023, s 27