VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DATA PROTECTION REGIME IN INDIAN LEGAL SYSTEM

- Snigdha Yelamanchili[1]

Abstract

The rapid digitization of governance, commerce, and social interaction has fundamentally altered the contours of privacy, necessitating a corresponding evolution in legal doctrine. In India, this transformation has been shaped by constitutional jurisprudence culminating in the recognition of privacy as a fundamental right, followed by legislative intervention through the Digital Personal Data Protection Act, 2023 (DPDP Act). This paper undertakes a doctrinal analysis of India's emerging data protection regime, situating the DPDP Act within the broader trajectory of privacy jurisprudence. It examines the shift from a fragmented, sectoral approach toward a consolidated statutory framework, while critically evaluating the Act's key principles—consent, mechanisms, legitimate use, data fiduciary obligations, right of data principles, and state exemptions. The analysis interrogates tensions between individual autonomy and state interests, particularly in the context of surveillance, data localization, and regulatory discretion. By mapping judicial reasoning against legislative design, the paper evaluates whether the current framework adequately safeguards informational privacy in a rapidly digitizing society. The paper concludes that while the DPDP Act represents a significant normative step forward, its operational effectiveness will depend on institutional safeguards, interpretive clarity, and judicial oversight. Ultimately, the paper contributes to understanding how India's privacy doctrine is being recalibrated in response to technological change and governance imperatives.

Key words: Data Protection, Privacy, Digital Personal Protection Act, Informational privacy, Constitutional Framework, IT Act 2000.

Introduction

In today's digital age, it's likely that you've sent an electronic message, made a phone call, filed taxes online, or

[1] Student at Amity Law School, Noida

utilized a smartphone, smartwatch, or fitness tracker. You may also shop online, use voice assistants like Alexa, or engage in various other internet-based activities. If you answered "yes" to any of these, then your personal information is being shared. While it's undeniable that these technologies have greatly benefited our lives, making everyday tasks more convenient and enabling us to stay connected with others, there's a trade-off involved. The data generated by our interactions with these devices and platforms reveals a wealth of information about us, including our personality, preferences, relationships, interests, and much more. This is where the importance of data protection and privacy comes into play. You might think that your online activities are harmless, but the reality is more complex. Your data can be used to create a detailed picture of your life, and this information can be vulnerable to exposure. It's essential to recognize the risks involved and take steps to safeguard your personal data and maintain your online privacy.[2]

It's undeniable that data has become a highly valuable commodity, often referred to as the new currency. As people go about their daily lives, they generate vast amounts of data, which has the potential to unlock new insights and opportunities. However, as data continues to grow in importance, several critical issues arise that require careful consideration. Who does the data belong to? Is it the individual who generated it, the company that collected it, or someone else entirely? Who has the right to access and control the data? Should it be the individual, the company, or government agencies? How can the data be used? Are there any limitations or restrictions on its use, and if so, who enforces them? How is privacy affected by the collection, storage, and use of data? Can individuals control their own data and maintain their right to privacy? As companies seek to harness the power of data to drive innovation and growth, they often encounter tension with individuals' right to privacy. The question is, can privacy serve as a limitation on how companies use data? The answer is complex and depends on various factors. Ultimately, striking a balance between data utilization and privacy is crucial. By acknowledging the value ofdata and addressing the complexities surrounding its ownership and use, we can work towards creating a more equitable and sustainable data ecosystem that respects individuals' rights while driving innovation and growth.

1.1 Indian Judiciary on Right to Privacy

Since 1960, Indian courts have addressed the right to privacy as a common law right as wellasaconstitutionallyrecognizedone.Thecourtshaveoptedtoevaluatesuchcaseson an individual basis, giving the right to privacy little weight.

In the case of *Kharak Singh v. State of UP*[3] the Supreme Court was instructed to give ruling on whether the police had the authority to monitor and visit people with criminal records. During their nightly visits, the police harassed the individual in question, in violation of Regulation 236(b) of the UP Police Regulation. The individual challenged them in court, claiming they violated his right to personal freedom.The judges objected because‘RighttoPrivacy’wasnotincludedamongthefundamentalrightsofpeople.Only twoofthesevenjudgessaidtheybelievedthattherighttoprivacyisstillabasicrightthat confers liberty,

[2] RakeshChandra,RighttoPrivacyin India WithReferencetoInformationTechnologyEra188(Mayur Printers, New Delhi, 2017).
[3]1964(1)SCR332

regardlessofwhether it isprotected bythe constitution. Judge Subba Rao decidedthat“Whiletherighttoprivacymaynotbeexplicitlystatedasafundamentalright in our Constitution, it is an integral part of personal liberty”.

In*Govindv. StateofMadhyaPradesh*[4], apetitioneronceagaincontestedpoliceactions on the grounds that they infringed upon his right to privacy. When it came to taking the right to privacy into account in an interpretation, the bench was divided once again. Accordingtothecourt,thegovernment shouldn'tmeddle inaperson'slifeunlessit would be unreasonable to do so. Judge Mathew decided that the Constitution protects people' rightsandliberties,guaranteeingthatnogovernmentagencymayviolatesomeone'sperson or property without a good reason.

Inthecaseof*(People'sUnionforCivilLiberties) PUCLv. UnionofIndia*[5],the legality of illegally listening in on phone calls was investigated. The court determined that it was against people'srighttoprivacytolisteninonphonecalls. Additionally,thegovernment's intelligence agencyisexpectedto tryto gather information inthis manner;nonetheless, it is essential to protect individuals' right to privacy from being abused by the existing authorities. Clearly, this would violate Article 21 of the Indian Constitution.

The Supreme Court took into consideration the right to privacy of the medical records of the blood donor in the case of *Mr. 'X' v. Hospital 'Z*[6]. Medical personnel have a moral and ethical duty to protect patient privacy due to the trusting nature of the doctor-patient relationship. Under some circumstances, one person's"right to be let alone"and another's "right to be informed" may clash under the Right to Privacy. Secrecy shouldn't be given prioritywhenthe public interestoutweighs the needto preserve anonymity, suchas when oneperson'sdiseaseendangersthehealthofothers.Inthisinstance,therespondinghospital disclosed the identity of a blood donor who had been diagnosed with HIV without the donor's permission. The blood donor's revelation led to his social exclusion and the dissolution of his engagement to his fiancée. The Supreme Court addressed the issue of medicalrecordprivacyinacase involvingthewife anddeterminedthat,ingeneral,medical recordsareprivate.Thecourtdidpointoutthatinsomeextraordinarysituationswhenthe patient'swife's life was indanger, hospitalsand physicians might deviate fromthis norm.

In the case of *District Registrar v. Canara Bank*[7], the Supreme Court rendered the historic ruling that affirmed the importance of privacy. If an examination of any public official's records, registers, books, or documents held by anypublic servant reveals fraud orthefailuretofulfillanyobligationowedtothegovernment,theCollectoror"anyperson" designated by the Collector may do so, according to the A.P. Stamps Act. Thus, the Supreme Court was asked to rule on the legality of the measure. The Supreme Court declared the challenged clause invalid because it failed to meet the rationality standards outlined in Articles 14, 19, and 21.

Therightto privacyprotects"privatespace inwhichmanmaystaywhat he is,"according totheDelhiHighCourt'sruling

[4] 1975SCC(CRI)468

[5](1997)1SCC30
[6]AIR1999SC495
[7](2005)1SCC496

inthe *NazFoundationcase*[8].As hedesires, heremains loyalto himself. The IndianConstitutionguaranteestheright to privacy, whichthe courts have construed as a fundamental aspect of human dignity. The court ruled that treating individuals with respect entails acknowledging themas important contributorsto society. Going beyond "place" into "person", the Naz Foundation promoted an impressive, non- spatial, and practical definition ofprivacy.Indian private culture is obviously influenced by elements like family rights, keeping the "purdah" (religion's fast), and the idea that meddling diminishes someone's modesty, dignity, or decency.

Indians have always seen privacy as a "societal value" rather than an "individual value," andthisvaluehasneverbeen"lessvalued"inIndianculture,asshownbylegalprecedents such as these.It demonstrates that Indians are more concerned with one facet of privacy and give that aspect's protection greater weight.In Indian civilization, privacy is seen as "essential" rather than a "contributory element." Although privacy is undoubtedly valued in Indian society, the level of respect for it varies from what we are used to in the West. Personalprivacy is not so mucha basic humanright as it is an issue of"respect" inIndia. ThemajorityofIndianprivacyregulationsarepracticalstandardsbasedon"socialethics", "virtues,"and"righteous"conduct.Thisperspectiveisconsistentwiththenation'scultural standards, which maintain that too much personal space prevents individuals from conversing and forming deep bonds with one another.

1.2 MeaningofthetermDataPrivacyandDataProtection

Understandingpersonaldataiscrucialbeforedelvingintothemeaningofdataprivacyand protection. This foundationalknowledge lays the groundworkfor adeeper understanding of these concepts.

Datacanbebroadlyclassifiedintotwo:

- **PersonalData**

personaldata is basicallyany information that can identify a specific person, whether it's their name, address, or something else. And the thing is, even if you combine different piecesofdata,itcanstillbeusedtoidentifythatperson.That'swhyGDPRdefinespersonal data as any information related to a living individualwho can be identified in some way.

- **Non-PersonalData**

Non-personaldataisbasicallyinformationthatdoesn'trevealtheidentityofanindividual. Evenifit'svaluable,it'snotconsideredpersonaldatabecauseitdoesn'tcompromise someone's privacy. Think ofcompanyregistrationnumbers, companyemailaddresses, or anonymized data - these are all examples of non-personal data.

Dataprivacyisastrategic imperative intoday'sdigitallandscape,wherepersonaldataisa valuable asset that requires protection from unauthorized access, misuse, or exploitation. It's about having controlover yourownpersonalinformation, deciding who getsto see it,

[8]NazFoundationvGovernmentofNCTofDelhiWP(C)No.7455/2001

shareit,anduseit.It'snotjustabouthandlingdataproperly,butalsoaboutrespectingyour righttoprivacy.Intoday'stech-savvyworld,yourpersonaldataislikeavaluableassetthat needs protection from unauthorized access. The notion of data protection is integrally associated with the treatment of personal data, concentrating on the just and lawful collectionandutilizationofsuchinformation.Theobjectiveofdataprotectionpoliciesand methodsistodiminishtheencroachment uponanindividual'sprivacybyguaranteeingthe conscientious management of their personal information. Data protection may be characterized as the juridical architecture that administers the accessibility and employment of data, with the aim of protecting personal data against abuse. This field includes both technical and administrative safeguards, the latter of which refers to the statutory components of data control.

While data security is necessary to create a safe environment for personal data, it is just onepieceofthepuzzle.Dataprivacyextendsbeyondsecurity,focusingontheresponsible and lawfuluseofdata.Forinstance,acompanymight employrobust securitymeasuresto protect user data from hackers but still violate privacy if they share this data with third parties without user consent. Therefore, effective data management requires a comprehensive approachthat integrates both dataprivacyand security. This involves not onlylocking downdatafromexternalthreats but also ensuring that internaldata handling practices respect individual privacy rights[9].

Privacyassuranceisunattainableinanenvironmentdevoidofsecurity,whilesecuritydoes not inherently implythe presence ofprivacy. Acomprehensive understanding of boththe differences and the nexus between data security and data privacy is fundamental. This understanding is a prerequisite for devising and applying definitive and meticulously formulated data security and privacy policies.

1.3EvolutionofDataProtectionLaws intheCountry

Thesafeguardingofindividualprivacyanddataisregulatedbyaspectrumoflawsrelated to information technology, criminal jurisprudence, intellectual property, and contractual agreements. The Planning Commission instituted a specialist group headed bythe retired JusticeA.P.Shahforthepurposeofcraftingfoundationalprinciplesaimedattheprotection of privacy rights.[10]

InformationTechnologyAct,2000

The InformationTechnologyAct of2000, complemented byits 2011 Rules, serves as the primary regulatory framework for the use and exchange of personal data.[11] The Act and its rules provide a legal framework for the

[9]Int'l Ass'nofPrivacyProf'ls, What DoesPrivacyMean?https://iapp.org/about/what-is-privacy(last visited March 2026).

[10]Press Information Bureau, SanctityofPersonal Data (2012), https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=88503.

[11] InformationTechnology(ReasonableSecurityPracticesandProceduresandSensitivePersonal Data or

handling, transfer, and usage of personaldata. WhiletheinitialpurposeoftheActwastoprotectelectronicinformationandregulateareas like cybercrime and e-commerce, reflecting itsrootsinthe 1996 UNCITRALModelLaw onECommerce,itsfocuswasnotprimarilyonprivacy.Nevertheless,the2008amendment, whichwasapprovedbythePresidentin2009,fortifiedtheActwithspecificdataprotection measures. These measures now require the enactment of privacy policies and enforce penaltiesintheeventofpolicybreaches.ThesectionsoftheActthatareapplicabletodata protection are as follow:

1. In accordance with Section 2(1)(o) ofthe Act, the term'data' refers to a varietyof entitiessuchas information, understanding, factualelements, and instructionsthat are structured or are to be structured. It is data that is slated for processing, is presentlybeingprocessed,orhasbeenprocessedinacomputersystemornetwork, oritisdatastoredwithinthecomputer'sownmemory.Itdoesnotdefinepersonal data.

2. As per Section 2(1)(v) of the Act, "information" is a term that captures a wide spectrum of items: this includes data, written messages, textual material, visual content, auditory recordings, spoken words, encryption methods, computer-based programs, software, electronic databases, and forms of microfilm or digitally created microfiche.[12]

3. In Section 43, there are various provisions that create civil liabilities for an individual who commits certain infractions, with the provision for awarding damagesto those affected bysuchactions. It isworthnoting that thissectiononly allows for compensation in cases where the individual has actually been affected by unauthorized activities such as access or disruption. It does not consider cases where the data subject might not have been directly affected but has had their privacy rights violated by such unauthorized access.

4. Section 43A, which was introduced as an amendment, serves as an important provision regarding the protection of data privacy. It mandates that any corporate body that possesses, deals with, or handles Sensitive Personal Information (SPI) via computer resources must establish and uphold suitable security practices and procedures.Thesectionspecifiesthattheremustbeanoccurrenceofwrongfulloss or

Information) Rules, 2011

[12] TheInformationandTechnologyAct,2000(Actof21of2000),s.2(1)(0).

wrongful gain to any individual in order for the corporate body to be held responsible for compensation.

Accordingtothecurrentprovision,acompanycannotavoidresponsibilitybyassertingthat it was not negligent in enforcing or upholding reasonable security measures. These reasonablesecuritymeasuresrefertothemethodsthatpreventunauthorizedentry,damage, use,change,exposure,orweakeningofinformation,asagreeduponbythepartiesinvolved oras required byexisting laws. Insituations where there is no suchagreement orspecific law, the centralgovernment isempoweredto establishthe requisite securitypracticesand procedures, doing so in collaboration with expert groups and industry associations.

The foundation of India's codified data protection laws is Chapter IX of the Information TechnologyAct.Section43AoftheInformationTechnologyActof2000imposesliability on the data controller in the case of a data breach.

Section43A:Compensationforbreachesofdata-Whenbusinessesnegligentlyneglectto put in place and maintain appropriate security standards and processes to safeguard sensitivepersonaldataorinformationheldintheircomputersystems,theyarelegally obligated to pay people.For individuals impacted, this may result in unjustified gain or loss. Reasoning. In the context of this section,

(i) "Body corporate" refers to any business, including sole proprietorships, firms, andotherassociationsofpeopleinvolvedinbusinessorprofessionalactivities;

(ii) "Reasonable security practices and procedures" refers to security measures intendedtopreventunauthorizedaccess,damage,use,modification,disclosure, or impairment of such information, as may be specified in a current law or in an agreement between the parties; in the absence of such a law or agreement, the Central Government may prescribe reasonable security measures and procedures after consulting with any professional bodies or associations it deems appropriate;

(iii) "Sensitive personal data or information" refers to any type of personal information that the Central Government determines it needs after consulting with pertinent professional groups.

Body corporates that handle, interact with, or hold sensitive data without proper security procedures seem to be subject to fines under this article. The concerned body corporate will be required to compensate the victim for any ill-gotten earnings or losses that result fromthis.One must consult the Indian Penal Code for advice on what qualifies as unfair gain.

It is evident from reading the wording at face value that liabilities would only be incurred against "body corporates,"which include companies, sole proprietorships, and other legal organizations. It is implied that the body corporates engaged in processing personal data were the main goal of the legislation's adoption since the punitive provision does not apply to individuals.

The computer resource used to process the data must be owned and controlled by a body corporate;

- The data must be categorized as sensitive.
- There must be proper security measures in place and the corporate body must not handle the data carelessly.
- Priority one should be given to the requirement that this negligence result in some kind of unfair gain or loss. The Indian legislature revised the Information Technology Act in 2009 to include section 74 A, which is intended to protect personal information in contractual agreements, along with a strict clause that attempts to prohibit breaches of personal information in non-contractual partnerships.

Section 43A omits any mention of 'Personally-Identifying Information,' and characterizes Sensitive Personal Data (SPD) in a restrictive manner. The section only extends a civil remedy under section 43A where there is a lack of due diligence by the corporation that leads to wrongful loss or gain to another party. Furthermore, the provision does not make any statements regarding its extraterritorial scope. Sections 43 and 43A also do not stipulate a maximum limit for compensation, a feature that has occasionally been misused by companies. Such misuse is seen in the form of spurious legal claims made by companies against former employees who have taken up positions with competitors in the same market space. Additionally, the Act includes provisions for a penalty or compensation as a catch- all response to instances of non-compliance with its directives.

1.4 Initiatives taken for Data Protection in India

As part of its efforts to improve data security, India has strengthened its data protection standards and strengthened its data security legislation. The Indian Ministry of Information Technology Act has made few attempts to raise the security threshold for data. One of these endeavors is the development of the STQC Directorate, which is supervised by the government under the DIT, or Standardization Testing and Quality Certification.[13]The Indian government has issued a statement in response to calls for Indian companies to adhere to stringent international security regulations.

[13]Anisha, Sanctity of Personal Data: A Comparative Study of Data Privacy Laws(2020),https://thelawbrigade.com/wp-content/uploads/2020/05/Anisha-IJLDAI.pdf.

The STQC Directorate offers testing and certification of software and hardware products, as well as training for employees on quality and security procedures. In addition, the Computer Emergency Response Team (CERT-In), which was also founded by DIT, is an essential part of India's data security architecture. CERT-In is accountable for ensuring that all information technology (IT) resources in India are free of malware and other security threats as a key member of the global CERT community. It handles computer security incidents centrally. System administrators and service providers are informed of best practices. Computer security and information security concerns are raised among internet users in India. issuing advisories and vulnerability notes to keep the community informed about the latest security threats, conducting research and development in collaboration with prominent research and educational institutions to tackle prevailing system security concerns and emerging cybersecurity challenges, connecting with similar international organizations, and acting as a hub for organizations to collaborate on addressing computer security issues. [14]

By taking these measures, India demonstrates that it is serious about enhancing national and international cybersecurity and data protection. All data collection and processing activities must be guided by the principles of equality and openness. It is important for individuals to know exactly why and how their data is being gathered. Data protection safeguards should also be in place at every stage of data's lifecycle, from collection to storage to transfer. For data protection policies and procedures to work, they need to be tailored to the specifics of each firm. Data security must be taught to staff members and made clear to them. They must comprehend the significance of adhering to all applicable regulations. It is of the utmost importance to safeguard any personally identifiable information and process it appropriately.

In addition to demonstrating ethical responsibility, this data collection strategy ensures compliance with GDPR and CCPA data protection standards. By lowering the likelihood of data breaches and abuse, it also contributes to the creation of a safer online environment. By carefully collecting data, businesses can generally better adapt to the evolving data privacy environment and lay the groundwork for ethical and long-term data management practices.[15]

Conclusion

[14]Anisha, Sanctity of Personal Data: A Comparative Study of Data Privacy Laws (2020),https://thelawbrigade.com/wp-content/uploads/2020/05/Anisha-IJLDAI.pdf.
[15]Jayanta Boruah & Bandita Das, *Right to Privacy and Data Protection under Indian Legal Regime* (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827766.

India's privacy jurisprudence has undergone a decisive transformation, moving from implicit constitutional protections to an explicit, rights-based framework that acknowledges informational privacy as central to individual dignity and autonomy. The Digital Personal Data Protection Act, 2023, marks a pivotal moment in this evolution, translating constitutional principles into a structured regulatory regime. However, the doctrinal analysis reveals that the Act embodies a careful—yet contested—balance between enabling data-driven innovation and safeguarding fundamental rights.

While the Act introduces important mechanisms such as consent-based processing, fiduciary accountability, and regulatory oversight, it simultaneously grants broad exemptions to the state and significant discretionary powers to the executive. This creates potential fault lines, particularly when assessed against the proportionality standards articulated in constitutional jurisprudence. The absence of an independent regulatory architecture with strong enforcement autonomy, coupled with ambiguities in key provisions, may dilute the robustness of privacy protection in practice.

The future trajectory of India's data protection regime will therefore hinge on how these tensions are resolved through judicial interpretation, regulatory practice, and possible legislative refinement. Courts are likely to play a crucial role in harmonizing the DPDP Act with constitutional guarantees, ensuring that privacy remains a meaningful and enforceable right rather than a formalistic promise. In this evolving landscape, the challenge lies not merely in enacting comprehensive legislation, but in sustaining a rights-oriented approach that can adapt to technological advancements without compromising democratic values.

In sum, the DPDP Act represents both an achievement and an inflection point—signaling progress in India's privacy framework while underscoring the need for continued doctrinal vigilance and institutional maturity.

Bibliography

Legislations/Statutes:

- TheConstitutionofIndia1950
- The Aadhaar(TargetedDeliveryofFinancialandOtherSubsidies,Benefitsand Services) Act, 2016, No. 18, Acts of Parliament, 2016. (India)
- IncomeTaxAct,1961

- IndianCopyrightAct, 1957
- IndianEasementAct, 1882
- IndianPenalCode,1860
- PublicFinancialInstitutions(ObligationastoFidelityandSecrecy) Act1983
- PublicRecordsAct,1993
- RighttoInformationAct, 2005
- TheCensusAct,1948
- TheCodeofCriminalProcedure, 1972

Rules and Regulations:

- InformationTechnology(IntermediaryGuidelinesandDigitalMediaEthicsCode) Rules, 2022
- InformationTechnology(Reasonable SecurityPracticesand proceduresand Sensitive Personal Data or Information) Rules, 2011
- ThePressCouncilofIndiaNormsofJournalisticConductrules,2010