ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

Data Protection Vis- A- Vis Right to Privacy

Nazuk Sood

Guru Nanak Dev University, Regional Campus, Jalandhar

DOI: https://doi.org/10.51244/IJRSI.2025.120600161

Received: 21 June 2025; Accepted: 24 June 2025; Published: 21 July 2025

ABSTRACT

Right to privacy is a fundamental right of every citizen as enshrined under Article 21 of the Constitution of India. In the digital age, where everyone is connected through the internet, data privacy is a myth. Individuals are sharing their personal data with each other while engaging in online shopping or accessing bank facilities on the internet, or sharing their details on social media platforms. The information that is available over the computer networks can be accessed by anyone and tampered with by anyone. The large collection of information on the internet is expanding at a rapid pace, and the spread of new technological innovations such as artificial intelligence and, internet of things has posed a threat of abuse and misuse of the data. It is the need of the hour to have a strong data protection regime. This paper discusses the need for data protection law in India and the constitutional status of the right to privacy in India. It also focuses on the existing legal framework about data protection and right to privacy in India. Also, the researcher has discussed the Joint Parliamentary Committee Report on the Data Protection Bill and the Digital Personal Data Protection Act, 2023.

Key Words: Right to Privacy, Data Protection, Data Fiduciaries, Information Technology, social media, Data Processing, etc.

INTRODUCTION

Privacy is not something that I am merely entitled to; it's an absolute prerequisite.

Marlon Brando

Privacy is one of life's basic requirements, which every person is entitled to. The right to privacy is inherent in every human being by birth. In general terms, the right to privacy refers to that right of an individual which enables him to regulate the collection, use and disclosure of the personal information. Personal information could be stored in the form of pictures, personal data such as educational background, family history or anything which could disclose a person's identity. Jude Cooley mentioned that "Right to Privacy is linked with the right to be let alone".[1] Right to Privacy protects individuals from the unwarranted intrusion of the government and other actors of society.

Right to Privacy has been recognised by various international instruments such as the Universal Declaration of Human Rights and International Covenants on Civil and Political Rights. Article 12 of this Declaration lays down that- "No one shall be subjected to arbitrary interference with his Privacy, family, home or correspondence, nor attacks upon his honour and reputation".[2] In India, the Right to Privacy has not been explicitly mentioned in the Constitution of India. It comes within the ambit of freedom of life and personal liberty enshrined under Article 21 of the Constitution.

Right to privacy is not only limited to the "right to be let alone" but can also be extended to other aspects such as personal freedom, data protection and confidentiality. Privacy is closely connected with the protection of data. They require that personal information about the individuals should be made accessible to other individuals or

[1] Cooley, "Thomas M. A Treatise on the Law of Torts", 29 (2nd ed, 1888).
[2] Universal Declaration of Human Rights, available at https://www.un.org/en/about-us/universal-declaration-of-human-rights(last visited on January 30, 2025)

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

organisations. The individual must be able to regulate the use of their data. Data protection is a legal safeguard to prevent the misuse of the information about the individual stored on any electronic medium.[3]

Constitutional Status of Right to Privacy in India

Right to Privacy has not explicitly mentioned as a fundamental right in the Constitution of India. The framework of right to privacy lies within the ambit of Article 21 which guarantees the right to life and person liberty to every person. Article 21 runs as "No Person shall be deprived of his life or personal liberty except according to the procedure established by law".[4] Through the various judicial pronouncements, the Court have recognised the right to privacy as a fundamental right which is implicit in "Personal Liberty" guaranteed under Article 21.

The issue whether the right to privacy is a fundamental right or not arose for the first time in the case of "Kharak Singh v. State of Uttar Pradesh"[5]. The main question which arose in this case was regarding the constitutionality of certain police regulations which allowed police to do domiciliary visits and surveillance of persons with criminal record. Petitioners challenged the domiciliary visits and surveillances by the police as unconstitutional as they are violative of the right to privacy as implicit under 'personal liberty 'of Article 21 of the Constitution of India. Majority if the Judges observed that "Right to Privacy does not lie within the ambit of the fundamental right to life and personal liberty as enshrined under Article 21 but the domiciliary visits into a person's house were unconstitutional". The dissenting view was expressed by Justice Subba Rao who recognised right to privacy as a fundamental right. He held that "It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty."[6]

In "M.P Sharma v. Satish Chandra"[7], the courts were to deliberate on the issue of constitutional restrictions which can be imposed on the government's power to exercise the right of search and seizure and whether such right infringes the right to privacy of an individual. The Court remarked that "The power of search and seizure is an overriding power of the State for the protection of social security and that power is necessarily regulated by law. Constitution makers did not expressly recognise the right to privacy as a fundamental right and there is no need at this stage to interpret right to privacy as a separate fundamental right".

In "Govind v. State of Madhya Pradesh"[8] the Supreme Court took a more elaborate approach towards the right to privacy. The Court observed that right to privacy flows from the fundamental right guaranteed under Article 19 (a), and 21 of the Constitution. But it cannot be made absolute. Like every other fundamental right, it is subject to the reasonable restrictions which can be imposed by the State. Similar observation was made by the Supreme Court in the case of "R. Rajagopalan v. State of Tamil Nadu".[9] The Apex Court held that right to privacy means right to be let alone. This right of privacy is implicit in the right to life and personal liberty as guaranteed under Article 21 of the Constitution. The Court expanded the scope of right to privacy and held that "A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing, and education among other matters. Publication of the above matters without the consent of the individual would amount to violating his right to privacy".

In "PUCL v. Union of India"[10], the Supreme Court observed that "Right to privacy lies within the ambit of right to life and personal liberty as enshrined under Article 21 of the Constitution. But such right is not absolute in nature. It can be curtailed according to the procedure established by law". But such procedure should be fair, reasonable, and not arbitrary.

[3] Singh, Shiv Shankar. "Privacy And Data Protection in India: A Critical Assessment." 53 Journal of the Indian Law Institute, 663, 2011.

[4] INDIA CONST. art 21.
[5] Kharak Singh v. State of Uttar Pradesh AIR. 1963 SC1295 (India).
[6] Ibid.
[7] M.P Sharma v. Satish Chandra AIR 1954 SC 300 (India).
[8] Govind v. State of Madhya Pradesh 1975 (3) SCR 946 (India).
[9] R. Rajagopalan v. State of Tamil Nadu 1994(6) SCC 632 (India).
[10] PUCL v. Union of India AIR 1997 SC 568 (India).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

Right to Privacy was given a new direction in the case of "Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors"[11]. The issue which came before the Apex Court was regarding the constitutional validity of the Aadhar Card Scheme. The main contention of the petitioner was that the mandatory collection and processing of biometric vitals of the individuals violates the fundamental right of privacy which is protected under Article 21 of the Constitution. 9 Judge Bench held that "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution. But this right is subjected to the restrictions imposed by Article 21. State can curtail the right according to the procedure established by law as mentioned under Article 21". In this case, the validity of the Aadhar card was upheld and Court remarked that the required disclosures under the Act does not violate individuals right to privacy. Moreover, the Court gave a new interpretation to right to privacy through this judgment and overruled the previous decisions that right to privacy is not recognised as a separate fundamental right which was laid in M.P. Sharma case & Kharak Singh case.

Right to privacy is not just restricted to the "right to be let alone". It has wide amplitude. It can also be extended to other aspects such as bodily integrity, personal freedom, data protection, protection from state surveillance, dignity, confidentiality, compelled speech, and freedom to express own opinions and thoughts. Tapping of telephone was always considered to the violation of the individual privacy. This issue has been considered by the courts in various cases. In **"**M. Malkani v. State of Maharashtra"[12]**,** the Supreme Court held that "Telephonic conversation of an innocent citizen will be protected by Courts against wrongful or arbitrary interference by the State by tapping the conversation. Telephone tapping is violative of Article 19(1)(a) and 21 of the Constitution".

Similarly in the case of "PUCL v. Union of India"[13] the Supreme Court observed that "Holding a telephonic conservation in the privacy of one's office or home without the interference can be claimed as a matter of right. Telephone tapping would attract the infringement of Article 21 of the Constitution of India". In "State of Maharashtra v. Bharat Shanti Lal Shah"[14] the Court held that "Interception of conversation would amount to invasion of privacy under Article 21. But such right is not absolute and can be curtailed according to the procedure established by law. The procedure itself has to be just, fair and reasonable and not arbitrary or oppressive".

Right to health is an important facet of right to privacy. In "Mr. X v. Hospital Z"[15], the question which arose before the Supreme Court was whether the disclosure by the doctor that his patient has been tested HIV positive would be violative of the patient's right to privacy. The Supreme Court ruled that "Right to Privacy like any other fundamental right is not absolute in nature and restrictions can be imposed for the prevention of crime, disorder, protection of health or morals and protection of other fundamental rights of others". The Court remarked that "Doctor was open to reveal such information to the girl whom he intended to marry as she had a fundamental right to know about the HIV- positive status of the appellant.

It is well established notion that like every other fundamental right, right to privacy is also not absolute in nature and reasonable restrictions can be imposed on such right by the State. In case there is a conflict between the fundamental rights of two parties, the right which favours the public morality would be given due preference. A three-judge bench in case of "Sharda v. Dharmpal"[16] ruled that "Court had the power to direct the parties to divorce proceedings, to undergo a medical examination. A direction issued for this could not be held to the violative of one's right to privacy as it would be covered within the ambit of the reasonable restrictions".

The right of privacy is broad enough to encompass the area of contraception and abortion, i.e., a woman's decision whether to terminate her pregnancy. The issue of abortion dominated the right to privacy for a long time. Through the various judicial pronouncements, it was laid down that the right to privacy signifies the right

[11] *Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors* 2017(1) SCC 1 (India).
[12] M. Malkani v. State of Maharashtra 1973(2) SCR 417 (India).
[13] PUCL v. Union of India AIR 1997 SC 568 (India).
[14] State of Maharashtra v. Bharat Shanti Lal Shah (2008)13 SCC 5 (India).
[15] Mr. X v. Hospital Z AIR 1995 SC 495 (India).
[16] Sharda v. Dharmpal AIR 2003 SC 3450 (India).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

of the individual to be free from intrusion into the matters fundamentally affecting a person as to decision whether to bear or beget a child.

In recent times, the Supreme Court has given the widest interpretation to the right to privacy by linking it with the rights of the LGBT Community. In "Naz Foundation v. Government of NCT of Delhi"[17] the Delhi High Court put more emphasis on the individual liberty and decriminalised Section 377 of Indian Penal code which talks about the unnatural offences. The Court held that "Treating consensual homosexual sex between adults as a crime is a violation of the fundamental right guaranteed under Article 21". But this decision was overturned by the Supreme Court in "Suresh Kumar Kaushal v. Naz Foundation"[18] The Court recriminalized Section 377 of Indian Penal Code. The Court held that consensual sexual intercourse among the same sex is against the order of nature and should be treated as a crime. But this decision of the court faced a lot of criticism and once again it was overturned by the Supreme Court in "Navtej Singh Johar v. Union of India"[19] The Court again decriminalised all consensual sex among adults in private including homosexual sex between the same gender. As a result of this judgment, Section 377 was declared unconstitutional in so far which criminalises consensual sexual conduct between adults of the same sex.

The scope of right to Privacy once again came before the judiciary while interpreting the law relating to adultery. The Court in "Joseph Shine v. Union of India"[20] , the Supreme Court decriminalized the adultery by striking down Section 497 of the Indian Penal Code. The Court observed that adultery is not an offence, and it should not be criminalised. Therefore Section 497 of the Indian penal Code was held unconstitutional. Further, the Court held that "Right to Privacy includes the autonomy of an individual to make their own sexual choices and it should be protected from the public censure through the criminal action".[21] Justice D. Y. Chandrachud stated that "Section 497 of the Indian Penal Code violated Article 21 of the Constitution as it does not provide dignity, liberty, privacy and sexual autonomy.

Now it is a well settled principle that Right to Privacy is a fundamental right which is a part of right to life and personal liberty as enshrined under Article 21 of the Constitution, Right to Privacy also includes the right to be forgotten and right to be left alone. Right to be Forgotten means the right to have publicly available personal information removed from the internet, search databases, websites, or any other public platforms once the personal information in question is no longer necessary or relevant.[22]

The Delhi High Court in "Jorawar Singh v. Union of India"[23] considered the issue of right to be forgotten. The petitioner who was an American citizen was charged under the Narcotics Drugs and Psychotropic Substances Act, 1985 but was later acquitted by the Court. The said judgment was published on the internet. Petitioners contended that details of his case could be found through a google search by any potential employer who wanted to run a background check on him before hiring. He filed a writ petition before the Delhi High Court requesting the websites to delete the said judgment as it was no longer relevant. The Court acknowledged the right to be forgotten and ordered the websites to remove the judgment from the websites. It was held that "Right to be Forgotten emerges from the right to privacy under Article 21 of the Indian Constitution"

Need for Data Protection in India

In general terms, Data refers to the "collection of information that is stored or processed in such a way that computers can easily read them". Data usually refers to information about an individual's messages, social media posts, online transactions, and browser searches. Data Protection refers to the safeguarding the personal data from its unauthorized use. In the age of digitalisation, every transaction or activity by the individual involves

17 Naz Foundation v. Government of NCT of Delhi 160 Delhi Law Times 277 (India).
18 Suresh Kumar Kaushal v. Naz Foundation 2014 (1) SCC 1 (India).
19 Navtej Singh Johar v. Union of India (2018) (India).
20 Joseph Shine v. Union of India (2019) 3 SCC 39 (India).
21 Adultery- Section 497 IPC , available at https://www.scconline.com/blog/post/2019/02/21/adultery-s-497-ipc-and-s-1982-crpc/ (last visited on February 2, 2025)
22 Right to be Forgotten, available at https://www.drishtiias.com/daily-updates/daily-news-analysis/right-to-privacy-right-to-be-forgotten (last visited on February 2, 2025)
23 Jorawar Singh Mundy v. Union of India, W.P. (C) 3918/ 2020

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

the data transaction. According to Section 2(1)(o) of the Information Technology (Amendment) Act, 2008, Data is defined as "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer"[24]

According to the Internet and Mobile Association of India (IAMAI's) Digital in India Report 2019, India has around 504 million active web users.[25] Due to such high active users all over India, sensitive data could be exposed with the stakeholders without the consent of the individuals. The landmark judgment in "K.S Puttaswamy" paved the way for the need of data protection law in India as right to privacy has been declared as a fundamental right by the Apex Court The unregulated and arbitrary use of data has raised serious concerns regarding the autonomy and privacy of the individuals. Recently, WhatsApp Accounts of 121 Indian Citizens were hacked by Pegasus an Israeli Software[26]. Without an effective data protection, there are increased chances of surveillance, profiling of individuals which is a direct attack on their right of privacy. Also, Information about the individuals and their online habits which have been shared on social media or stored on a computer network has become an important source of profits for many companies and advertising agencies. Without any proper regulations of data norms in India, we are providing the large personal information about the individuals to the foreign companies.

In recent times, India has witnessed a radical change in the increasing of the cybercrimes. Hackers are difficult to trace as they are extremely organised and collaborative in exposing the personal information of the individuals. Moreover, the large collection of the information on the internet is expanding at a rapid pace and spread of the new technological innovations such as artificial intelligence, internet of things has posed a threat of abuse and misuse of the data.[27] Therefore, it is the need of the hour to have a strict mechanism for the data protection in India.

Legislative Framework for Data Protection in India

There is no proper legislative regime for the data protection in India. There is no specific legislation which exhaustively deals with the protection of data. However, the Information Technology Act, 2000 deals with the transactions which are carried through the electronic data interchange and electronic communication. The Act contains provisions to safeguard the data from the unauthorized use of computer systems or networks. Section 43 of the said Act provides that "Where any person without the permission of the owner or any other person who is in in-charge of the computer, computer system or computer network accesses, downloads any information or introduces any virus on computer system or cause any damage to the data or computer network and deletes or tamper with the information stores in a computer resource shall be liable to pay damages by way of compensation not exceeding 1 crore rupees to the affected party."[28]

Section 72 of the Information Technology Act, 2000 talks about the breach of confidentiality and privacy. It provides that "Any person who has secured access to any electronic record, book, information, document or other material without the consent of the person concerned discloses such electronic record, book, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both". [29]

[24] The Information Technology (Amendment) Act. 2008, Section 2(1)(o).
[25] Data Protection in India, available at https://www.drishtiias.com/daily-updates/daily-news-analysis/data-protection-in-india (last visited on February 7, 2025)
[26] Data Protection in India, available at https://www.digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf(last visited on February 7, 2025).
[27] Data Protection Bill 2019, available at https://d19k0hz679a7ts.cloudfront.net/value_added_material/The_Personal_Data_Protection_Bill_2019.pdf(last visited on February 8, 2025).
[28] Information Technology Act, 2000, Section 43.
[29] Information Technology Act, 2000, Section 72.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

Compensatory rights are available against the improper disclosure of the personal information under the Information technology (Amendment) Act, 2008. Section 43 A of the said Act provides for the compensation in case of the failure to protect the data. It mentions that "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected."[30]

Section 72 A which has been added by the Amendment Act of 2008 provides for the punishment for disclosure of the information in breach of the lawful contract. It mentions that "Any person including an intermediary who while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both".[31]

The Information Technology Act, 2000 only provides the power to the authorities to monitor and collect the data. "Personal Data" has not been defined under the Act anywhere. The Act also lacks in the mechanism of the data quality obligations in relation to sensitive data or personal information. Moreover, it does not impose any kind of obligations on private sectors to disclose the details of the practices in handling and managing the content or personal information stored over the internet. [32]

Personal Data Protection Bill, 2018

Pursuant to the decision of the Supreme Court in K.S Puttaswamy v. Union of India which holds that right to privacy is a fundamental right of the citizen, the Government appointed a committee headed by Justice B. N Srikrishna to examine the issues linking the privacy and data protection and to propose a draft legislative framework relating to the data protection. The Committee drafted a Bill popularly known as "Personal Data Protection Bill, 2018." The Bill has laid out the framework for data protection and mentions the limits for the collection and processing of personal data of the individuals.

The main objective of the Bill is to create the accountability and prevent the unauthorized use of the sensitive data available on the computer networks. The Bill is applicable to both the Government and Private sectors. The aim is to provide the individuals the control over their personal data. The individuals must give explicit consent to process their personal information, and they must be notified by the private authorities. Since the right cannot be made absolute, the Bill also provides the extent of government regulations over certain kinds of data. Government can access and control the information for reasonable purposes such as "national security, whistleblowing, unlawful activity, health services and legal proceedings, etc."[33] The Act also provides for the establishment of a national-level Data Protection Agency for supervising and regulating the private entities. It also mentions the stiff penalties in case of the misuse of the data.

Personal Data Protection Bill, 2019

To overcome the shortcomings in the Draft Protection Bill of 2018, the Parliament revised the Bill, and it was named as Personal Data Protection Bill, 2019. The purpose of the Bill is to ensure the protection of the personal data of individuals and establish a Data Protection Authority for the same. Data is categorised under 3 heads under the Personal Data Protection Bill, 2019[34]

[30] Information technology (Amendment) Act, 2008, Section 43 A.
[31] Information technology (Amendment) Act, 2008, Section 72A.
[32] Supra note 3
[33] Privacy and Data Protection in India, available at https://www.mondaq.com/india/privacy-protection/1148288/privacy-and-data-protection-in-india-2021-wrap?type=popular(last visited on February 9, 2025)
34 Personal Data Protection Bill, 2019, available at https://prsindia.org/billtrack/the-personal-data-protection-bill-2019 (last visited on February 9, 2025).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

Personal Data – It identifies the personal details of the individuals such as name, address, and identity of a person

Sensitive Personal Data - It relates to the finances, health, sexual orientation, Biometric, genetics or the religious beliefs of the individual

Critical Personal Data – It is concerned with the information related to national or military security.

The Personal Data Protection Bill 2019 applies to the Government Companies incorporated in India and Foreign Companies that deal with the personal data of individuals in India. Data fiduciaries are entities that decide the purposes for processing the personal data. Personal Data can be processed only for a clear, lawful, and legitimate purpose. All the data fiduciaries must undergo the transparency and accountability measures while processing the data. They are bound to implement the security safeguards, such as data encryption, to prevent the misuse of the data. Also, a grievance redressal mechanism can be opted for to address the complaints of the individuals. These entities must also institute the mechanisms for age verification and parental consent when processing sensitive personal data of children.[35]

The Bill provides certain rights to the individual to ensure the data privacy. These include[36] –

Right to obtain the confirmation from the fiduciary about the processing of the personal data

Right to rectify the inaccurate, incomplete, or outdated personal data

Right to restrict the disclosure of the information if it is no longer necessary or relevant.

The Bill also mentions that "Data Processing is based on the notion of the consent, and it is allowed only when the individual gives the consent for the same. Provided that the personal data can be processed without the consent if it is required by the State for the benefits of the individuals or in medical emergencies or it is required for the legal proceedings". [37]

The Bill provides that the Central government can exempt its agencies from the provisions of the Bill in the interest of the security of the state, public order, sovereignty and integrity of India and friendly relations with foreign states, and for preventing incitement to the commission of any cognizable offence. Also, stricter penalties are mentioned for violation of the provisions of the Bill. It states that "Processing or transferring personal data in violation of the Bill is punishable with a fine of Rs 15 crore or 4% of the annual turnover of the fiduciary, whichever is higher"[38]

Joint Parliamentary Committee Report on Personal Data Protection Bill, 2019

Recently, Joint Parliamentary Committee have revised the Personal Data Protection Bill, 2019. It recommended the following changes to be made to the existing Personal Data Protection Bill, 2019[39] –

The scope of the Privacy Bill should be extended to the non -personal data as well.

Data Localisation should be encouraged. The Committee suggested that "Government should bring back mirror copies of all sensitive and critical personal data already stored abroad".

Social Media should be made accountable in case the privacy of the individual is compromised. Report points out that "All Social Media Platforms must be held accountable for the content they launch and mandates the

[35] Ibid.
[36] Mandeep Kumari, & Puja Kumari, Data Protection and Right to privacy: Legislative Framework in India, 7 Journal of Critical Reviews, 2020. 0
[37] Supra Note 34.
[38] Supra Note 36.
[39] JPC Report on PDP Bill, available at https://www.drishtiias.com/daily-updates/daily-news-analysis/jpc-report-on-the-pdp-bill(last accessed on February 9, 2025)

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

verification of the accounts through ID verification of every user.". This is done to safeguard against the various fake accounts and bots on social media.

The Committee retained Section 35 of the Personal Data Protection Bill, which provides that "Government can exempt any of its agencies from the provisions of the Act for the processing of the personal data. These exemptions include the "Interest of the security of the state, sovereignty and integrity of India, public order and friendly relations with foreign states, and to prevent incitement to the commission of any cognizable offence."

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Bill, 2023, received presidential assent on August 11, 2023. The previous Personal Data Protection Bills from 2019 and 2022 were withdrawn by the Central Government due to several amendments and issues regarding data localisation, transparency, and compliance. The primary objective of this Act is to create a comprehensive framework for the protection and processing of personal data. It applies to the processing of personal data in India, including both online and digitised offline data. Furthermore, it extends to the processing of such data outside India when it relates to the offering of goods or services in India.[40]

This Act defines "Data" as any representation of information, facts, concepts, opinions, and instructions that is capable of being communicated, interpreted, and processed by human beings or by automated means. Further, any data about an individual who is identifiable by or in relation to such data has been referred to as Personal Data in the Act. This Act does not apply to the personal data when such data is processed by an individual for any personal or domestic purpose, and is made or caused to be made publicly available by the Data Principal herself or any other person under an obligation to make such Personal Data publicly available.

It has been provided in Section 6 of the Act that Personal Data may be processed only for the specified purpose and after obtaining the consent of the individual. Such consent has to be free, specific, informed, unconditional, and unambiguous. Moreover, notice under Section 5 of the Act must be given by the Data Fiduciary before seeking consent, containing details about the Personal Data to be collected and the purpose of processing. The individual whose data is being processed can withdraw her consent at any time. For individuals with disabilities or below eighteen years of age, the Act provides that their consent will be provided by their parents or legal guardians.[41]

This Act also discusses the rights and duties of the data principal in detail. It provides that an individual whose data is being processed shall have the following rights –

Can obtain information about processing

Seeking correction and erasure of Personal Data

Nominating another person to exercise rights in the event of death or incapacity

Withdrawing consent at any time during or after the processing of Personal Data.

Further, Section 15 of the Act states that the Data Principals will be under an obligation not to register a false complaint or suppress any material information while providing their personal data; and furnish any false particulars or impersonate in specified cases. The breach of said duties will attract a penalty as per the Schedule to the Act.

This Act also provides for the obligations of a data fiduciary. Section 8 of the said Act provides that the data fiduciary must process the personal data only for which the consent has been provided by the data principal or for a certain legitimate use. He must make reasonable efforts to ensure the accuracy and completeness of data and implement appropriate measures to protect Personal Data in his possession or under his control. Moreover,

[40] Ishwar Ahuja, "Digital Personal Data Protection Act, 2023- A Brief Analysis", available at https://www.barandbench.com/view-point/digital-personal-data-protection-act-2023-a-brief-analysis (last visited on March 1, 2025).
[41] Ibid.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

he must inform the Data Protection Board of India and affected persons in the event of a personal breach, and erase Personal Data as soon as the purpose has been met.

According to Section 17 of the Act, the provisions related to 'Obligations of Data Fiduciaries' and 'Rights & Duties of Data Principal' have been made inapplicable in specified cases, which include:

Prevention, investigation or prosecution of offences

Enforcement of legal rights or claims

Processing to ascertain financial information, assets, and liabilities.

Processing of Personal Data by the State or any other instrumentality of the State in the interest of the security and public order, and necessary for research, archiving, or statistical purposes.

In addition to this, Section 29 of the Act provides that "The appeals against the decisions of the Board shall lie with the Telecommunications Dispute Settlement and Appellate Tribunal (TDSAT) established under the Telecom Regulatory Authority of India Act, 1997. The appeal shall be preferred within sixty days from the date of receipt of the Board's decision. Furthermore, the Schedule to the Act lays down the quantum of penalties to be imposed for various offences and breaches committed under the Act. The penalties will be imposed by the Board after conducting an inquiry under Section 33.

Shortcomings of the Act

With the introduction of this new Act, companies and businesses that handle Personal Data in any capacity will be required to develop standard operating procedures and train their personnel to comply with specific regulations. This includes cooperating with the Data Protection Officer appointed by the Significant Data Fiduciary as per Section 10 of the Act, hiring an Independent Data Auditor, implementing a consent management mechanism to collect, maintain, track, and update consent from individuals, conducting assessments to protect data, and maintaining valid contracts with data processors, among other requirements. However, the criteria for classifying companies and startups as Data Fiduciaries need clarification, particularly concerning thresholds and eligibility criteria such as net worth, assets, size, number of personnel, and their qualifications.

While the Act appears to prioritise the protection of Personal Data, there are concerns regarding the technical implementation of its provisions. For example, Section 36 grants the Central Government the authority to request "such information" from the Board or any Data Fiduciary or intermediary. This broad power and vague terminology, when examined, suggest an underlying intent for surveillance by the Central Government. Furthermore, Section 17(2)(a) allows the Central Government to exempt any instrumentality of the State from certain provisions concerning the processing of Personal Data.

Additionally, Section 8(1)(j) of the Right to Information Act, 2005 has been amended by Section 44(3) of this Act. This amendment could disrupt the balance that the RTI Act sought to achieve between privacy and the right to information, as it appears to broaden the powers of a Public Information Officer. Now, such an officer can deny applications made under the RTI Act because the requested information pertains to Personal Data.

CONCLUSION

The intersection of data protection and the right to privacy represents one of the most critical challenges of the digital age. As personal data becomes a valuable asset in governance, commerce, and technology, ensuring individual autonomy and dignity through effective legal safeguards is both a constitutional imperative and a moral necessity. The recognition of the right to privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India not only affirmed the centrality of privacy in a democratic society but also underscored the urgent need for a robust, rights-based data protection framework.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue VI June 2025

While legislative efforts such as India's Digital Personal Data Protection Act, 2023, are commendable steps toward aligning domestic law with global privacy standards, the true effectiveness of such frameworks depends on their implementation, oversight, and respect for due process. A rights-oriented approach to data protection must ensure transparency, accountability, proportionality, and user empowerment, particularly in the face of increasing state surveillance and corporate data monetisation.

Ultimately, data protection must be seen not merely as a regulatory obligation but as a constitutional guarantee that upholds the sanctity of the right to privacy. The road ahead requires continuous judicial vigilance, policy reform, and public awareness to ensure that technological advancement does not erode the fundamental freedoms that form the bedrock of a constitutional democracy.