PROTECTING PRIVACY IN THE AGE OF CONNECTIVITY

Author: Treasa George, II year of LL.M from Government Law College, Ernakulam.

ABSTRACT

In the contemporary era defined by ubiquitous connectivity and the seamless exchange of information facilitated by the internet, the notion of privacy has undergone a profound transformation, presenting Complex challenges and opportunities. This paper embarks on an exploration of the dimensions of privacy protection in the digital age, with a particular focus on the legal frameworks and notable cases within the Indian context. Central to this discourse is the recognition of privacy as a fundamental right, enshrined and upheld by the judiciary. Delving into landmark cases, the paper elucidates the evolution of privacy jurisprudence in India. It underscores the judiciary's pivotal role in interpreting constitutional provisions to safeguard individual autonomy and personal liberty against encroachments from state and non-state actors alike. Furthermore, the paper analyses the legislative arsenal deployed to fortify privacy protections, ranging from provisions within the Indian Penal Code to the Information Technology Act. Of particular significance is the scrutiny afforded to the Digital Personal Data Protection Act, 2023, a pivotal legislative milestone designed to usher in a new era of data and privacy protection. Through an examination of its provisions, including the delineation of rights and duties of data principals, the paper elucidates the Act's potential in harmonizing individual privacy rights with the imperatives of data-driven innovation and economic growth.

INTRODUCTION

In the age of the internet, where information flows freely and connectivity knows no bounds, the concept of privacy has taken on new dimensions and challenges. As the world becomes increasingly interconnected, individuals find themselves navigating through both physical and virtual spaces, each with its own set of privacy concerns. The rise of technology has ushered in an era where personal data is constantly being collected, analysed, and utilised, often without explicit consent or knowledge.

Privacy, defined as an individual's right to control his or her personal activities or intimate personal decisions without outside interference, observation and intrusion,[1] has become a critical issue in today's globalized society. It encompasses both physical privacy, involving protection from intrusion into one's physical space or solitude, and digital privacy, which pertains to the collection and use of user information in the online realm.

The advent of the internet has facilitated unparalleled access to information and communication channels, revolutionizing the way individuals interact and share ideas. However, it has also led to the proliferation of digital footprints, consisting of a trail of data generated by users during their online activities. This data, comprising both active and passive digital footprints, is often harvested by companies and utilised for various purposes, including targeted advertising and predictive analysis. The implications of this vast collection of personal data are profound, raising concerns about privacy infringement and the potential for misuse by both companies and malicious actors.

LEGAL DIMENSIONS OF PRIVACY PROTECTION

With the advent of the Internet, it has become easy for anyone to get, compile and exploit the private information of individuals.[2] What were scattered, unimportant, small bits of data has now become a potent large set of data that can be misused by companies or by antisocial elements. This has prompted many countries to come up with legislation on privacy.

As basic principles for the protection of privacy there are three international treaties that are widely recognized as the basis for the protection of privacy and personal life such Article 12 of the Universal Declaration of Human Rights, and Article 17 of the International Covenant on Civil and Political Rights. The OECD guidelines on the Protection of Privacy and Trans border Flow of Data are also of relevance in this aspect.[3]

[1]Black's Law Dictionary (10th ed. 2014).
[2]AshwinMadhavan& Rodney D Ryder, *Internet Law* (2018).
[3]KeyurTripathi, *Protection of Privacy in Cyberspace: A Comparative Analysis Between India and* USA (2020).

THE RIGHT TO PRIVACY: A FUNDAMENTAL RIGHT

The Constitution of India does not expressly grant the fundamental right to privacy. However, the courts have read the right to privacy into the Right to Life and Personal Liberty under Article 21.

The case **MP Sharma v. Satish Chandra**[4] related to search and seizure of documents of some companies following investigations into its affairs. In this case, the Supreme Court decided in favour of the practice of search and seizure when contrasted with privacy.

The right to privacy was invoked in the case **Kharak Singh v. State of Uttar Pradesh and Others**[5] to challenge the surveillance of an accused person by the police. Kharak Singh was arrested for dacoity but was released due to a lack of evidence. The Uttar Pradesh Police subsequently brought him under surveillance, which was allowed under Chapter XX of the Uttar Pradesh Police Regulations. Kharak Singh then challenged the constitutional validity of Chapter XX and the powers it conferred upon police officials, as it violated his fundamental rights under Article 19(1)(d) (right to freedom of movement) and Article 21 (protection of life and personal liberty). The 6-judge bench held that domiciliary visits at night was unconstitutional, but upheld the rest of the Regulations. More importantly, the bench held that the right of privacy is not a guaranteed right under the Constitution.

In **R. Rajagopal v. State of T.N.,**[6] popularly known as "Auto Shanker case" the Supreme Court has expressly held the "right to privacy", or the right to be let alone is guaranteed by Art. 21 of the Constitution. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, childbearing and education among other matters. No one can publish anything concerning these matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right of the person concerned and would be liable in an action for damages. However, position may be differed if he voluntarily puts into controversy or voluntarily invites or raises a controversy.

In the matter of **People's Union for Civil Liberties v. Union of India,**[7] commonly known as telephone tapping cases, the Supreme Court held that individuals had a privacy interest in the

[4] 1954 AIR 300, 1954 SCR 1077.
[5] 1963 AIR 1295, 1964 SCR (1) 332.
[6] (1996) 2 SCC 549.
[7] AIR 1997 SC 568.

content of their telephone communications. The Supreme Court has held that telephone tapping is a serious invasion of an individual's right to privacy, which is part of the right to life and personal liberty enshrined under article 21 of the Constitution, and it should not be resorted to by the state unless there is public emergency or interest of public safety requires.

In **Justice K.S. Puttaswamy v. Union of India**[8], the constitutional validity of Aadhaar was challenged on the ground that it violated the right to privacy of an individual. It was contended that Aadhar posed a serious threat to an individual's privacy by compromising their bodily integrity as it required the collection and storage of biometric information for authentication (fingerprints, iris scans), opening up possibilities of misuse. Further, the collection of personal information also heightened the risks regarding data security, coupled with dangers associated in relation to data storage and data breaches. A 9 Judge Bench of the Supreme Court delivered a unanimous verdict, affirming that the Constitution of India guarantees each individual a fundamental right to privacy. It was held that the requirement under the Aadhaar Act to give one's demographic and biometric information does not violate the fundamental right to privacy. The Court directed the Union Government to set up a data protection regime, for safeguarding individual interests in relation to infringement of privacy. Pursuant to the judgment, the government formed a committee of experts under the leadership of Justice B.N Srikrishna to consider all issues related to data protection and come up with a draft legislation thereon.

In**Karmanya Singh Sareen v. Union of India,**[9] thepetitioners challenged WhatsApp's 2016 privacy policy, claiming it posed a threat to Indian users' data privacy. Despite WhatsApp's initial assurance that the policy wouldn't change after its acquisition by Facebook in 2014, the company announced a new policy in 2016, allowing data sharing with Facebook and its affiliates.ThePublic Interest Litigation was filed with the prayer to prohibit WhatsApp from sharing, in any manner, details and data of every user of WhatsApp with any entity including Facebook or its family of companies; It was contended by the petitioners that the action of taking away the protection to privacy of details and data of users of WhatsApp and sharing the same with "Facebook" and all its group companies for the purpose of commercial advertising and marketing amounts to infringing the fundamental rights of the users guaranteed under Article 21 of the Constitution. The Delhi High Court directed WhatsApp to delete data of users choosing to uninstall the app and so far as the users who opt to remain in

[8] (2017) 10 SCC 1.
[9] W.P.(C) 7663/2016.

WhatsApp are concerned, the existing data of such users up to 25th September 2016 shall not be shared with Facebook or any one of its group companies

In January 2021 WhatsApp introduced a new privacy policy, which was met with public resistance, leading to an extension of the acceptance deadline to May 15, 2021. The petitioners alleged that the introduction of payment services on WhatsApp mobile application, it had increased the range of data it collects to include sensitive financial information. WhatsApp imposed new privacy policy on its users which enables it to share the personal and financial information with third parties, who provide no services to WhatsApp users, and who may further share the information to whom they please. It was further alleged that the European users of WhatsApp have the option to deny WhatsApp the use of their personal and financial information, however, the same courtesy is not extended to the Indian users.

The Division Bench of the Supreme Court[10] took note of an undertaking given to the Ministry of Electronics and Information Technology, Government of India, on 22nd may 2021. WhatsApp had given the undertaking that its users in India who have not yet accepted the 2021 privacy policy would not face any disruptions in using the application. It also directed WhatsApp to abide by the undertaking till the next date of the hearing. The Supreme Court as an interim direction directed WhatsApp to give publicity in 5 national newspapers on two occasions with full-page advertisement which should necessarily contain the undertaking.

In the next hearing, the Supreme Court took note of the submission by the Attorney-General that the Digital Personal Data Protection Bill, 2022 which addresses the issues in the case is going to be tabled during the monsoon session of the Parliament. So it was directed that a Bench can be constituted after the bill has been passed.

THE INDIAN PENAL CODE, 1860[11]

The IPC contains provisions for various offences related to privacy, such as voyeurism and stalking under Sections 354C and 354D. Section 354C states that any individual who observes or captures the image of a woman engaging in a private act in circumstances where she would reasonably expect not to be observed, and then disseminates such image, shall be

[10] Petition(s) for Special Leave to Appeal (C) No(s). 804/2017.
[11] The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).

punished upon first conviction with imprisonment for a term not less than one year but which may extend to three years, along with a fine. On a second or subsequent conviction, the punishment includes imprisonment for a term not less than three years but which may extend to seven years, in addition to a fine. Section 354D defines stalking as the act of a man repeatedly following or attempting to contact a woman despite her clear disinterest, or monitoring her electronic communication. However, certain exceptions apply. Stalking is not considered a crime if it was done to prevent or detect crime, and the accused was entrusted with such responsibilities by the State. It's also not considered a crime if it was done to comply with any legal requirement or condition imposed by any person. Furthermore, the conduct is deemed reasonable and justified in the specific circumstances. Punishment for stalking varies depending on the conviction. On the first conviction, the punishment includes imprisonment for up to three years and a fine. On the second or subsequent conviction, the punishment escalates to imprisonment for up to five years and a fine.

THE INFORMATION TECHNOLOGY ACT, 2000[12]

Data security breaches, such as those committed by individuals hacking into computer systems could result in the prosecution of offenders under Sections 43 and 66 of the Information Technology Act.

According to **Section 43**, if anyone, without permission, accesses or helps others access a computer, computer system, or network, copies data from it, or assists in such actions in violation of the IT Act, will be liable to pay compensation to the affected person for the damages caused.

According to **Section 66**, if any person, dishonestly or fraudulently, does any act referred to in Section 43, shall be punishable 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.

Initially, the IT Act did not provide a remedy against the organization responsible for a breach of data. Subsequently, Section 43A and Section 72A were retrospectively added to the Act for this purpose by the amendment in 2008. Section 43A provides that a body corporate shall be liable to pay damages by way of compensation to the person affected by a breach of

[12] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

data protection, owing to actions of such body corporate, while Section 72A states that any person, including intermediaries, who, while providing services under a lawful contract, gains access to material containing another person's personal information and discloses it to someone else with the intent to cause wrongful gain or loss, without consent or in violation of the contract, may face penalties. Penalties may include imprisonment for up to three years, a fine of up to five lakh rupees, or both.

Section 66E of the Act specifies that anyone who intentionally or knowingly captures, publishes, or transmits an image of a person's private area without their consent, thereby violating their privacy, may face imprisonment for a term that can extend to three years or a fine not exceeding two lakh rupees, or both.

According to **Section 72** of the IT Act, save as otherwise provided in the IT Act or any other law for the time being in force, if a person who, in pursuance of any of the powers conferred under the Act or rules gains access to electronic records, books, correspondence, or other materials and without the consent of the person concerned discloses them to someone else, they shall be punished with imprisonment for up to two years, a fine of up to one lakh rupees, or both.

Section 69 of the Act empowers the Central Government or a State Government, or their authorized officers, to intercept, monitor, or decrypt information in a computer resource if they believe it is necessary in the interest of India's sovereigntyor integrity, defence, security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of any cognizable offence relating to above or investigating certain offenses. Additionally, the subscriber, intermediary, or the person in charge of the computer resource must provide all necessary facilities and technical assistance when requested by the authorized agency to access, intercept, monitor, or decrypt information stored in the computer resource.

Section 69B of the Act allows the Central Government to authorize a government agency to monitor and collect traffic data or information from computer resources to enhance cyber security and prevent the spread of computer contaminants. Intermediaries or those in charge of computer resources must provide technical assistance and facilities for online access to the data as requested. Intentional contravention of these provisions by an intermediary may result in imprisonment for up to three years and a fine.

THE INFORMATION TECHNOLOGY (REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION) RULES, 2011 ("IT RULES, 2011")

The IT Rules, 2011 provide for the protection of sensitive personal data or information by body corporates. The rules prescribe certain security practices and procedures that must be followed while collecting, storing, and using personal data.

Under the provisions of the IT Rules, 2011, certain compliances are applicable in respect of a "body corporate", defined as including "company, firm, sole proprietorship or other association of individuals engaged in commercial or professional activities" which dealt in the collection, disclosure, and transfer of "personal information" and "sensitive personal data or information".

The IT Rules, 2011 defined "personal Information" as meaning "any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person".[13] and "sensitive personal data or information" as including personal Information relating to "passwords; financial information such as Bank Account or Credit Card or Debit Card or other payment instrument details; physical, physiological and mental health condition; sexual orientation; medical records and history; Biometric information; etc. any detail relating to the aforementioned as may be provided to the body corporate for providing service; and any of the information received by the body corporate under the aforementioned for processing, stored or processed under lawful contract or otherwise.". However, "any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force" is not considered sensitive personal data or information.[14]

Rule 4 of IT Rules directs body corporates collecting, receiving, or storing information, to provide a privacy policy for dealing with personal information and to guarantee that the same can be viewed by the providers of such information. This Rule further directs the body corporate or any person on its behalf to publish on the website the statements, type, the purpose of collection, and, the reasonable security practices employed by the former. **Rule 5** provides that the collection of information by a body corporate shall be done only after

[13] Rule 2(i).
[14] Rule 3.

obtaining consent in writing from the provider of the information. **Rule 6** provides that disclosure of sensitive personal data or information by the body corporate can only be done after obtaining the consent of the provider of the information unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation. **Rule 7** lays down that a body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021

These rules prohibit and regulate digital media and content on the internet, and the role of intermediaries, including social media intermediaries, in keeping the personal data of their users safe online. In particular, these require all intermediaries to publish on their websites and mobile applications all rules and regulations, privacy policy[15] and user agreement for access or usage of their online resources by any user as well as available mechanisms for grievance redressal[16], including the name and details of a grievance officer.[17] Additional compliance is prescribed for significant social media intermediaries such as Twitter, Facebook etc.[18]This includesappointing a Chief Compliance Officer who shall be responsible for ensuring compliance with the IT Act and rules made thereunder, publishing periodic compliance report every month mentioning the details of complaints received and action taken thereon, etc.

[15] Rule 3(1) (a).
[16] Rule 3(2).
[17] Rule 3.
[18] Rule 4.

DIGITAL PERSONAL DATA PROTECTION ACT, 2023[19]

In July 2017, the Ministry of Electronics and Information Technology appointed a 10-member Committee, under the chairmanship of Justice BN Srikrishna, to submit a detailed report on privacy and draft the Personal Data Protection Bill. The committee tabled its report on the need for new data protection law in India, accompanied by the draft Personal Data Protection Bill, 2018. The draft Bill sought to regulate the flow and usage of personal data and various entities processing the personal data, create a framework for accountability, processing of data, cross-border transfer and provide remedies for contravention. Prominently, it sought to establish a Data Protection Authority of India for the said purposes.

The Personal Data Protection Bill was largely modelled after the European Union's **General Data Protection Regulation**. After various rounds of amendment in 2019 and 2021, the bill was scrapped and replaced with the **Digital Personal Data Protection Bill**. The Digital Personal Data Protection Bill was passed by the Lok Sabha on 7th August 2023 and by the Rajya Sabha on 9th August 2023. The bill received the Presidential assent on 11th August 2023.

The Digital Personal Data Protection Act, 2023 provides for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes.

According to the Act, "data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;[20]

The Act applies to the processing of digital personal data within India, whether collected in digital or non-digital form and digitized later. It also applies to processing digital personal data outside India if it's related to offering goods or services to Data Principals within India. A "Data Principal" means the individual to whom the personal data relates to. In the case of a child, the definition includes the parents or lawful guardian of that child and in case of a person with a disability, it includes their lawful guardian who acts on their behalf.[21]

[19] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[20] Section 2h.
[21] Section 2 j.

However, the act does not apply to personal data processed for personal or domestic purposes or data made publicly available by the Data Principal or under any Indian law.[22]So for example, an individual, while blogging her views, has publicly made available her personal data on social media. In such case, the provisions of this Act shall not apply.

According to **Section 4**, a person can process a Data Principal's personal data only according to the provisions of the Act and for a lawful purpose, for which the Data Principal has given her consent or for certain legitimate uses.

The Data Principal has the right to withdraw their consent at any time. The process for withdrawing consent should be as simple as the process for giving consent initially.[23] The consequences of the withdrawal shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal.

A Data Fiduciary, who is the person or persons responsible for determining the purpose and means of processing personal data, must delete personal data:

1. When the Data Principal withdraws their consent. or
2. When it's reasonable to assume that the specified purpose for which the data was collected is no longer being served, except when retention is required to comply with existing laws.[24]

If a Data Principal has given consent for their personal data processing before the enactment of the Act, the Data Fiduciary must, as soon as reasonably possible, provide the Data Principal with a notice containing: (i) the personal data and the purpose for which the same has been processed; (ii) the manner in which she may exercise her rights under the Act and (iii) the manner in which the Data Principal may make a complaint to the Data Protection Board.[25]

The Act also places on the entities responsible for collecting, storing, and processing digital personal data the obligation to maintain security safeguards; to ensure completeness, accuracy, and consistency of personal data; as well as to intimate data breach to the Data Protection Board of India. The consent of the parent/guardian is mandatory in the case of

[22] Section 3.
[23] Section 6(4).
[24]Section 8(7).
[25] Section 5(2).

children or a person with a disability. The Act also states that any processing that is likely to have a detrimental effect on a child is not permitted. The Act also prohibits tracking, behavioural monitoring, and targeted advertising directed at children.

According to **Section 10** of the Act, the Central Government may notify certain Data Fiduciaries as "Significant Data Fiduciaries" based on the volume and sensitivity of personal data they handle, risks to data principle's rights, impact on India's sovereignty and integrity, risks to electoral democracy, national security, and public order.

Significant Data Fiduciaries have certain responsibilities, including appointing a Data Protection Officer based in India, who represents the Significant Data Fiduciary and acts as the point of contact for grievance redressal. Also, an independent data auditor to assess compliance with the Act should be appointed. The Significant Data Fiduciary should also conduct periodic Data Protection Impact Assessments, which involve assessing the rights of data subjects, the purposes of data processing, and managing risks as well as carry out periodic audits.

Chapter III of the Act deals with the rights and duties of the data principle

The Data Principal has the right to request from the Data Fiduciary:

1. A summary of the personal data being processed by the Data Fiduciary, along with the processing activities related to that data.
2. The identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared, along with a description of the shared data. and
3. Any additional information regarding the personal data and its processing, as prescribed by law.

According to Section 12, a Data Principal shall have the right to correct, complete, update and erasure of her personal data for the processing of which she has previously given consent.

A Data Principal shall also have the right to have readily available means of grievance redress provided by a Data Fiduciary.[26]

[26]Section 13.

A Data Principal also has the right to appoint another individual, as prescribed by law, who will be authorized to exercise the Data Principal's rights under the Act in case of the Data Principal's death or incapacity.

These are some of the rights enjoyed by the data principal. Now moving on to the duties of the data principal:

According to **Section 15**, the data principal has the duty to

a) Adhere to all relevant laws while exercising rights under the Act.

b) Duty to avoid impersonation when providing personal data for a specific purpose.

c) Duty to ensure that they do not withhold material information when providing personal data for any government-issued document, unique identifier, proof of identity, or proof of address.

d) Duty to refrain from registering false or frivolous complaints with a Data Fiduciary or the Board.

e) Duty to provide only information that is verifiably authentic when using the right to correction or erasure under the Act.

Section 17 of the Act provides exemptions from consent and notice requirements in certain cases like:

(a) Where processing is necessary for enforcing any legal right or claim; (b) personal data has to be processed by courts or tribunals, or for the prevention, detection, investigation, or prosecution of any offenses; (c) where the personal data of non-Indian residents is being processed within India; and so on.

In addition, the law exempts certain purposes and entities completely from its purview. These include:

1. Processing by such instrumentality of the State as the Central Government may notify in the interests of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order, or preventing incitement to any cognizable offense. This will allow investigative and security agencies to remain outside the purview of this law.

2. When Data processing is necessary for research, archiving, or statistical purposes and if the personal data is not to be used to make any decision specific to a data principal is also exempted.

3. The government can also exempt certain classes of data fiduciaries, including startups, from some provision like notice, completeness, accuracy, consistency, and erasure.

The Act provides for the establishment of the Data Protection Board of India. The Board shall consist of a Chairperson and such number of other Members as the Central Government may notify. The Board is empowered in case of personal data breach to issue urgent remedial or mitigation measures in response to the breach, investigate the breach, and impose penalties.

Any person aggrieved by an order or direction made by the Board may prefer an appeal before the Appellate Tribunal.

CHALLENGES TO THE RIGHT TO PRIVACY IN LIGHT OF THE ENACTMENT OF DIGITAL PERSONAL DATA PROTECTION ACT, 2023

- **Section 17(5)** allows the government to, "before expiry of five years from the date of commencement of this Act," declare that any provision of this law shall not apply to such data fiduciary or classes of data fiduciaries for such period as may be specified in the notification. This is a significant and wide discretionary power and is not restricted by any guidance on the basis for such exemption, the categories that may be exempted, and the time period for which such exemptions can operate.
- According to **Section 17(2)** the provisions of the Digital Personal Data Protection Act shall not apply in respect of the processing of personal data— (a) by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it;

  This means that consent of an individual is not required when the State processes personal data. Exemptions to data processing by the State on grounds such as national security may lead to data collection, processing, and retention beyond what is necessary. This may

violate the fundamental right to privacy. Since data taken for various purposes could be combined, this could allow the profiling of citizens. On the other hand, if consent were required, individuals would have the autonomy and control over collection and sharing of their personal data.

- The Act allows the transfer of personal data outside India, except to countries notified by the central government[27]. This mechanism may not ensure adequate evaluation of data protection standards in the countries where the transfer of personal data is allowed.
- The Act does not provide for the right to data portability. The right to data portability allows data principals to obtain and transfer their data from data fiduciary for their own use, in a structured, commonly used, and machine-readable format. It gives the data principal greater control over their data. It may facilitate the migration of data from one data fiduciary to another. Individuals can decide to move their data from one service to another, ensuring that they are not locked into a single platform or provider.
- The members of the Data Protection Board of India will be appointed for two years and will be eligible for re-appointment. The short term may affect the independent functioning of the Board.

CONCLUSION

The rapid advancement of technology and the proliferation of digital platforms have brought about significant changes in the realm of privacy protection. In the age of connectivity, where information is readily accessible and personal data is constantly collected, stored, and processed, ensuring the protection of individual privacy has become paramount.

Across the globe, nations are grappling with the challenge of striking a balance between harnessing the benefits of technological innovation and safeguarding the fundamental right to privacy. Legal frameworks and regulations play a crucial role in addressing these concerns, providing guidelines for the collection, storage, and use of personal data while also outlining penalties for violations.

In India, the evolution of privacy laws has been marked by significant judicial pronouncements and legislative initiatives. From recognizing the right to privacy as a fundamental right under the Constitution to enacting comprehensive legislation like the

[27] Section 16.

Digital Personal Data Protection Act, 2023, the country has taken significant strides in safeguarding individual privacy rights.

The Digital Personal Data Protection Act, 2023, with its emphasis on consent, transparency, and accountability, represents a significant milestone in India's privacy framework. By establishing clear guidelines for data processing, imposing obligations on data fiduciaries, and providing mechanisms for grievance redressal, the Act seeks to instill confidence among individuals regarding the protection of their personal data.

However, as technology continues to evolve and new challenges emerge, the journey towards ensuring robust privacy protection is an ongoing endeavour. It requires continuous adaptation of laws, proactive enforcement mechanisms, and collaborative efforts between governments, businesses, and civil society.

BIBLIOGRAPHY

- Alan Davidson, The Law of Electronic Commerce (2011).
- Annapurna Trivedi, UpendraNath Tiwari, Mridul Bhatt, Data Protection and Privacy Concerns in Cyberspace (2023)

  https://ijariie.com/AdminUploadPdf/DATA_PROTECTION_AND_PRIVACY_CONCERNS_IN_CYBERSPACE_ijariie18990.pdf
- AshwinMadhavan& Rodney D Ryder, Internet Law (2018).
- Carly Nyst, Two sides of the same coin – the right to privacy and freedom of expression (2018) https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression
- FarzadDamania, the Internet: Equalizer of Freedom of Speech? a Discussion on Freedom of Speech on the Internet in the United States and India, Vol. 12:2 IND. INT'L & COMP. L. REV.(2002) https://mckinneylaw.iu.edu/iiclr/pdf/vol12p243.pdf
- J.N. Pandey, Constitutional Law of India (2017).

- PRS India, The Digital Personal Data Protection Bill, 2023, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023#:~:text=The%20Bill%20does%20not%20regulate,notified%20by%20the%20central%20government.

- Rachna Sharma & Pradeep Kumar, Internet and Freedom of Speech (2016) https://loksabhadocs.nic.in/Refinput/New_Reference_Notes/English/FINAL_INTERNET_and_FOS.pdf