INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 2 | Issue 3 [2024] | Page 249- 265

© 2024 International Journal of Legal Studies and Social Sciences

Follow this and additional works at: https://www.ijlsss.com/

In case of any queries or suggestions, kindly contact editor@ijlsss.com

CYBER SHIELD EVOLUTION

- **Sushmitha. J**[1]

ABSTRACT

Almost two decades ago, India's data protection landscape was uncharted territory. The exponential growth of digital economy and increasing concerns about breaches prompted the government to take decisive action. Data is indeed powerful on its own, but it needs the aid of the law to be regulated.

The evolution of data protection in India has undergone significant transformations, particularly in response to the rapid digitalization and increasing concerns over privacy and data security.

Starting with the first comprehensive legal framework, the journey began with basic privacy protections embedded in the constitution and various statutes, such as The Information Technology Act of 2000.

The landmark Supreme Court judgment in 2017 recognizing the right to privacy as fundamental right marked a pivotal moment, prompting calls for more robust protection regime.

Furthermore, in 2022 Digital Personal Data Protection bill, which replaced its predecessor and introduced significant changes, including a shift from rights-based to risk-based approach based on these analysis highlights the implications of these changes for businesses, individuals and digital ecosystem as well as provides an overview of historical context and future implications of data protection in India, highlighting the critical need for a cohesive strategy to protect personal information in the digital age.

Ultimately, this article provides a comprehensive narrative of India's data protection evolution, offering insights for policymakers, legal practitioners and industry navigating this rapidly changing landscape.

Keywords: Data protection, Privacy, Digital rights, Cyber Security, Laws and legislations

[1] BBA.LL.B.

OBJECTIVE

The study is based on critical analysis on evolution Of Data protection in India in this regard following objectives are taken into consideration:

- Tracing evolution of data protections
- Contemporary issues and challenges faced in field of Data protection.
- To study legal provisions and legislations made relating to Data protection in India.
- To do a detailed study on the concept of Data Protection Bill and its relation with Data Privacy in India.

RESEARCH METHODOLOGY

All data and information present in this research paper are collected from various reports which are been prepared by national and international information's and collected from several authentic websites and journals relating to Data protection. The study is evaluated on the basis of reviewing several articles and books.

INTRODUCTION

- There were more than 13.9 lakh cyber security incidents in India in 2022, according to government reports.
- Data of over 100 million Flipkart, Airtel, Amazon, and Jiomart customers were sold on the dark web for $6,000.
- Razorpay, an online payment gateway, lost 7.3crore worth of funds in 831 transactions as hackers stole them.

With an intensely digitalized world and an increasingly digitalized India, the significance assumed by the data has reached unprecedented heights in the last couple of decades. The motive behind most of the cyber security attacks in India in the recent past has been aimed at stealing data. There have been numerous instances of health data, financial data and other important personal[2] and sensitive data being compromised by the cyber attackers[3]. according to the Indian Computer

[2] PAVAN DUGGAL, CYBER SECURITY LAW 42-103 (1ST ED. 2019)

[3] Jason Asbury, Maria McClelland, Kris Torgerson, India Vincent & Jennifer Boling, Law and Business Technology: Cyber Security & Data Privacy Update, 20 Transactions: TENN. J. BUS. L. 1065, 1067-71 (2019).

Emergency Response Team (CERT-In), there has been a significant increase in data breaches in recent years. In 2020, India witnessed a 300% increase in cyber-attacks. India's journey towards a comprehensive data protection law began in the early 2010s. The rapid growth of the internet and the burgeoning digital economy highlighted the need for a framework to protect individuals' personal data from misuse.

DATA PROTECTION

Data Protection has been defined as one of the most abstract concepts in the law that is bereft of being ascribed a one-line definition. Jurists have opined that the term "data protection" is a catch-all terminology that is used to denote everything that is associated with the processing of personal data[4]

HISTORY

"The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data"[5]. Indeed India's aspirations to be a knowledge economy coupled with the very real issues faced in cases of data being transferred to and processed in India particularly by the services sector has made it necessary for India to craft a clearly thought out policy in respect of data protection.

Historically, the concept of data protection and privacy were not addressed specifically in any Indian legislation. In the absence of a specific legislation, the Supreme Court of India has in a number of decisions recognized the "right to privacy" as a subset of the larger "right to life and personal liberty" under Article 21 of the Constitution of India[6]. However a right under the Constitution can be exercised only against any government action. Non-state initiated violations of privacy may be dealt with under principles of torts such as defamation, trespass and breach of confidence, as applicable.

---

[4] David Wallace & Mark Visger, Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community, 6 J.L. & CYBER WARFARE 3, 12-13 (2018).

[5] Preface to OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.html

[6] Kharak Singh v State of UP, AIR 1963 SC 1295; People's Union of Civil Liberties v. the Union of India, (1997) 1 SCC 318

The Information Technology Act, 2000 ("IT Act") is the only legislation which has attempted to address the issue of data protection. There are two basic elements of data protection under the IT Act.

The first concerns negligence in maintaining reasonable security practices and procedures to safeguard specific items of information classified as sensitive personal data or information which can identify a natural person ("SPDI"), where such negligence results in wrongful loss or wrongful gain to any person. The Government has in 2011 introduced certain rules ("India Data Protection Rules") under the IT Act which, read along with Section 43A, which set out the compliances which need to be observed by an entity which collects or stores or otherwise deals with SPDI. The second element is in relation to intentional disclosure of any personal information of any person that is capable of identifying such person, including any SPDI ("Personal Information") which has been collected under a contractual relationship.

On analysis of various other laws and guidelines dealing with data protection, it appears that there is a commonality of purpose for most laws and guidelines dealing with data protection.

Section 43(a) and section 66 of the act provides guidelines on breaches and penalties for unauthorized access. Additionally, the rules governing the protection of personal data were laid down in IT (Reasonable security practices and procedures and sensitive personal data or information)rules, 2011.

JUDICIAL ACTIVISM (2017)

The Supreme Court of India, in a landmark judgement in August 2017 in Justice K.S. Puttaswamy (retd) vs.. Union of India[7]- recognized the right to privacy as a fundamental right under Aricle-21 of the constitution. The judgement significantly heightened the discourse around personal data protection and privacy in India

[7] (2019) 1 SCC 1

DATA PROTECTION BILL (2019)

The B N Sri Krishna Committee had laid the foundation of the beginning of an era of the establishment of a comprehensive code on the data protection regime in India[8]. The Narendra Modi government last year appointed a committee under the chairmanship of Justice (Retd.) B.N Srikrishna, which has been tasked with the mandate of proposing measures to effectively address issues around data protection and privacy. The lacunas in the existing laws relating to the absence of incorporation of the key data protection principles and the need to have a more extensive and data principal centric law had led to the formation of the committee to suggest the roadmap for a new and comprehensive data protection legislation. The 10-member committee led by Honorable Justice B N Sri Krishna; a former judge of the Supreme Court of India submitted its report containing the recommendations for a comprehensive data protection regime in India along with a draft data protection bill[9]. The recommendations mirrored the provisions of the GDPR to a great extent and provided for the adoption of the key data protection principles in the Indian legal arena. At the time of its release, the draft bill had been hailed as the foundation of the core principles of the upcoming data protection regime in India[10].

The draft bill had defined the key aspects of data protection regime including the meaning of data[11], processing[12], the personal data[13], sensitive data[14] much on the lines of the GDPR. Then it provided restricted grounds on which the personal data of the individuals may be processed by the state and the corporations[15].

The bill had also pitched for stringent data localization norms while providing that at least one copy of the data sought to be transferred across the borders has to be stored in India. The draft bill had also pitched for a broad meaning of the rights of the data principal and recognized, the

[8] Justice Srikrishna Committee Submits Report On Data Protection. Here're Its Top 10 Suggestions, The Economic Times. (July 2020.) <https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-committee-submits-report-on-data-protection-herere-the-highlights/articleshow/65164663.cms?from=mdr> [Accessed 28 May 2020].
[9] Id.
[10] Meity.gov.in. 2020. WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA. <http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf> [Accessed 28 May 2020].
[11] Sec. 12 Personal Draft Data Protection Bill 2019.
[12] Sec. 29 Personal Draft Data Protection Bill 2019.
[13] Sec. 32 Personal Draft Data Protection Bill 2019.
[14] Sec. 35 Personal Draft Data Protection Bill 2019.
[15] Sec. 40 Personal Draft Data Protection Bill 2019

right to data portability, the right to be forgotten[16], the right to accessibility[17]and the right to correction[18]. Further, the draft bill had laid a great deal of emphasis on the importance of informed consent[19]

The Committee's report was subjected to a lot of criticisms, ranging from having pushed the need to protect the informational privacy of the citizens at a backseat while giving primacy to the economic aspects of the personal data[20] It also drew fire from the academicians and right to information activists for its flawed composition. The members of the committee consisted of the personalities that had been vocal in support of the Aadhar Act and had even at various point of times, opposed the recognition of the right to privacy as a fundamental right[21].

ONGOING DEBATE AND AMENDMENTS

The proposed personal data protection bill has undergone multiple rounds of discussions and public consultation. However, it also faced criticism regarding data localization clauses, government surveillance provisions, and potential over reach. Later in 2021, a new version of bill was released, which attempted to address some of these concerns, leading to further discussion among stakeholders.

DATAPROTECTION AUTHORITY(DPA)

The proposed bill envisaged the establishment of a data protection authority to oversee and enforce data protection regulations, ensuring compliance and addressing grievances. However, as of now, this authority is yet to be formally instituted pending the finalization of the bill.

"The Reserve Bank of India (RBI) reported over 8,000 cyber security incidents in 2020, with the majority affecting the banking sector".

[16] Sec. 27 Personal Draft Data Protection Bill 2019.
[17] Sec. 24 Personal Draft Data Protection Bill 2019.
[18] Sec. 25 Personal Draft Data Protection Bill 2019.
[19] Sec. 02 Personal Draft Data Protection Bill 2019.
[20] Why India's Proposed Data Protection Authority Needs Constitutional Entrenchment, The Wire (2021), https://thewire.in/tech/india-data-protection-authority-needs-constitutional-entrenchment (last visited Feb 24, 2021).
[21] The Data Protection Bill only weakens user rights, The Hindu (2021), https://www.thehindu.com/opinion/lead/the-data-protection-bill-only-weakens-user-rights/article30405339.ece (last visited Feb 24, 2021).

The GDPR and the DPDP Act are pretty comprehensive legislations that have quite a few similarities between them. The provisions that are similar in both of them are as follows:

Provisions	General Data Protection Regulation(GDPR)	Digital Personal Data Protection Act (DPDPA)
Personal data	Article 4(1) defines the term as any information that may directly or indirectly relate to an identified natural person.	Section 2(t) define as any data by the virtue of which an individual may be identified.
Extent	Article 3 of the regulations spells out the applicability of the GDPR to establishments even outside the European Union. Also, the GDPR has extra territorial jurisdiction and applies in respect of European citizens, residents and institutions that have a presence in the EU.	Section 3, the Act is applicable to digital data alone and not for offline personal data or non-automated processing of personal data.
Data collection and processing	Article 5 - personal data of an individual be collected only for lawful, fair and transparent reasons. Furthermore, Article 6 states the situations in which the processing would be considered to be lawful.	Section 4 of the Act states that for any processing of the data to be in accordance with the Act, it needs to be done for lawful purposes for which the data principal has given consent. Section 5 requires a notice to be given to the Data Principal regarding what information being collected and for what purposes. Section 7 states, the Data Fiduciary may process the personal data of the data principal if voluntary consent has been provided in respect of the same or provide to the Data Principal subsidy, benefit, licence or permit as prescribed under the section.

Data minimization	The principle of data minimization was introduced for the first time in the GDPR. Article5-The personal data collected shall be adequate, relevant and limited to what is actually necessary and in relation to the purpose of the collection.	No similar provision.
Consent	GDPR predominantly relies on consent to verify if data has been collected and processed lawfully or unlawfully. Consent in these cases would be considered valid only when it's freely given, clear, affirmative and capable of easy withdrawal. Article7-provision to withdraw consent .	Section 7, elaborates on the requirements of valid consent. consent seems to be freely given, informed, specific, and unambiguous, and it must indicate the data principal's wishes regarding the processing of the data.
Rights of individuals	The first legislation that accorded rights to data subjects. Article 15- the right to request information from the data controller about what personal information has been collected and uses. Article 16- right to rectify any inaccurate or incomplete data. Article 17 of these regulations allows the data subjects to erase their personal data when it is no longer required and has served the purpose for which it was collected. The right to restrict the processing of personal data has been enshrined in Article 18. By virtue of Article 20, the people also have a right to request a copy of their	Following the path of the GDPR, the DPDP Act has granted people a bunch of rights. Section 11, grants the Data Principal's right to information about their personal data. He has a right to obtain information about the processing of his personal data, summary of the data being processed, categories of data shared or other information as needed. Section 12, The right to correct and erase personal data when it's no longer required or for the purpose for which it was collected. Section 13 states the right to avail grievance redressed as soon as possible. Section 14, the right to nominate.

	personal data, and that too in a readable format. Article 21, the data subjects can also object to the processing of their personal data.	
Assessment	Article 35, It states that if any business does any work involving high risk to data privacy, then need to conduct a impact assessment. It is mandatory when business is involved in automated decision making, or processing special categories of information or criminal records or is monitoring in a public area.	Section 10, not every Data Fiduciary is required to appoint a data protection officer. Only a Significant Data Fiduciary is required to go through the process of appointing a Data Protection Officer.
Role of data controller	Article 24 states that a data controller has the responsibility of ensuring compliance with the GDPR. Article 25 similarly imposes a duty on the data controller to ensure use of adequate data protection measures and safeguards to protect the data.	Section 8 prescribes the general obligations of the data fiduciary. Obligated to protect the personal data and take reasonable security safeguards to prevent any breach of the data. He is bound to appoint a data processor. In case any breach occurs, should give notice of such to the Board in the manner and form as prescribed.
Penalties	In case organisations do not comply with the regulations, they can be fined up to 4% of their global turnover or €20 million, whichever is greater.	Section 33, the data protection authority can impose penalties on organisations if they fail to comply with the Act. penalty may be up to 5% of their annual turnover or Rs. 500crores, whichever is higher.

KEY PRINCIPLES OF THE DPDPA

The DPDPA is based on six key principles:

- Lawfulness: Personal data must be processed lawfully, fairly, and transparently.
- Purpose Limitation: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Data Minimization: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy: Personal data must be accurate and, where necessary, kept up to date.
- Storage Limitation: Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Integrity and Confidentiality: Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures

RIGHTS OF DATA PRINCIPALS

- The right to access their personal data.
- The right to rectification of inaccurate personal data.
- The right to erasure of their personal data.
- The right to restrict the processing of their personal data.
- The right to data portability.
- The right to object to the processing of their personal data.

NEED FOR DATA PROTECTION

A survey by Data Security Council of India (DSCI) revealed that over 87% of Indian consumers are concerned about their data privacy.

India is going through a digital transformation where people are using technology and the internet more and more in their daily lives. As a result, the necessity for cybersecurity and data protection measures to protect people and businesses from cyberattacks and data breaches has increased. India is the second-largest internet market in the world, with an estimated population of 1.3 billion, and is anticipated to expand quickly.

India has come a long way from the days when the concept of data protection as confined to the narrow walls of the Information Technology Industries. As noted, the use of data has become an indispensable aspect of the Indian economy and hence there is need of a comprehensive framework that would cater the needs of data protection in India.

PENALTIES AND FINES FOR VIOLATING DATA PROTECTION LAWS

Chapter 8 of the DPDP Act deals with penalties and adjudication. Section 33 provides that the Board will impose a monetary penalty after concluding an inquiry on the breach and after giving the person concerned a reasonable opportunity of being heard.

The amount of compensation as per Schedule 1:

Subject matter	Section of the DPDP Act	Penalty
Failure to take reasonable security safeguards to prevent personal data breach	Section 8 (5)	May extend to Rs. 250 crores
Failure to notify the board and affected Data Principals of a personal data breach	Section 8 (6)	May extend to Rs. 200 crores
Non- fulfilment of additional obligations in relation to processing of data of children	Section 9	May extend to Rs. 200 crores
Non- fulfilment of additional obligations of significant data fiduciary	Section 10	May extend to Rs. 150 crores
Violation of user duties	Section 15	May extend to Rs. 10,000

Breach of any term of voluntary undertaking accepted by the board	Section 32	Up to an extent applicable for beach in respect of proceedings were instituted under Section 28
For all other non-compliance under the Act	Every other section	May extend to Rs. 50 crores

EMERGING CHALLENGES AND FUTURE DIRECTIONS

With the rise of new technologies such as AI, Blockchain and the internet of things(IOT), challenges regarding data privacy and protection are increasingly complex. The Indian government and various stakeholders must continuously adapt to protect citizens data while also fostering innovation.

RECENT DEVELOPMENTS (2023)

As of 2023, the government of India is expected to finalize the personal data protection bill, aiming to create a robust regulatory framework. This development is critical not just for individual privacy rights but also for India's growing digital economy, while increasingly relies on data driven technologies.

CASES

- M.P. Sharma v. Satish Chandra (1954): One of the first cases in India that dealt with the right to privacy in India. An eight judge bench of the highest court of the land sat down to decide upon the constitutionality of the search and seizure provisions of the Code of Criminal Procedure. The Court here doesn't recognise any right to privacy and held that the search and seizures weren't, in fact, violative of the right to privacy. As there is no provision in the Indian Constitution that deals with the right to privacy, it can't be violated as well[22].

[22] M. P. SHARMA AND OTHERS vs. SATISH CHANDRA, DISTRICT MAGISTRATEDELHI, AND OTHERS. [1954] 1 S.C.R. 1077

- Kharak Singh v. State of UP[23]: The Apex Court decided in relation to privacy rights. It examined wide powers of police surveillance and its overarching powers in relation to privacy. Here, the Court for the first time, was faced with issues pertaining to the right to privacy as a part of Article 21. The court didn't explicitly recognise any right to privacy, but J. Subba Rao stated in his dissent that the right to privacy is inherent in our Constitution. This famous dissent helped initiate the growth of the right to privacy.
- This is the decision where the Supreme Court was again faced with a similar question of right to privacy. The facts of the case were such that it dealt with police surveillance by domiciliary visits. The Supreme Court recognised the significance of the right to privacy but said that it should give way to a larger state interest. It states that the right to privacy has its own set of restrictions, such as public order, morality, national security, etc[24].
- The Hon'ble Court, speaking through a bench of seven judges, said that the term 'personal liberty' includes a variety of rights within its ambit. The rights so recognised must fulfil the triple test, that is, they must prescribe a procedure; that procedure must follow the test of fundamental rights under Article 19 and also withstand the tests of Article 14[25].
- Another landmark decision in 1997 was decided in favour of the right to privacy. The case centred around telephone tapping of people without their consent and whether doing so infringed on their right to privacy. It was a PIL filed against rampant phone tapping by the CBI. The Court disallowed such phone tapping without consent, stating that it is an important facet of Article 21. The Court declared that doing so amounts to a rather serious infringement of the right to privacy. In declaring the same, the Court marked an important step in the journey of protection of the right to privacy[26].
- In R. Rajagopal v. State of Tamil Nadu[27], where the Apex Court recognised the right to privacy of prisoners as well. More popular than the 'Auto Shankar case', it allowed the prisoner the right to publish his autobiography without any restrictions. In declaring the same, the court emphasised on the right to be left alone and, more particularly, to be in jail. This also includes an individual's right to control the dissemination of

[23] [1964] 1 SCR 332, AIR 1963 SC 1295
[24] Govind vs. State of Madhya Pradesh & Ors AIR 1975 SC 1378, (1975) 2 SCC 148
[25] Maneka Gandhi v. Union of India, AIR 1978 SC 597
[26] People's Union for Civil Liberties vs. Union of India & Ors. AIR 1997 SC 568, (1997) 1 SCC 301
[27] AIR 1995 SC 264, (1994) 6 SCC 632

information regarding their private life and the power to control any unwarranted intrusion into their rights.

- In this case, court was faced with a clash between two different fundamental rights: the right to privacy on the one hand and the right to public morality on the other. The appellant was a patient whose diseases were announced in public by the hospital. The Court recognised the right to privacy in such circumstances, stating that every person has a right to life and a healthy lifestyle under Article 21. It was mentioned that disclosure of even true private facts has the capability of breaching someone's peace of mind and privacy[28].
- Another case, where the Hon'ble Court rules on the significance of financial privacy of an individual. It stated that the right to privacy also extends to maintaining the confidentiality of bank account details and related information as well. This decision basically widened the scope of the right to privacy and also covered the financial aspects of the right[29].
- The Naz Foundation v. Government of NCT of Delhi (2009)[30] , The Delhi High Court turned out to be a significant development on the issue of consensual homosexuality. The Court gave its verdict on the validity of Section 377 of the Indian Penal Code, 1860. The Court ruled that Article 21 also protects a person's right to become whoever he wants and to remain himself. They said that all individuals need a place of sanctuary where they can be free from societal expectations. Then this case was overturned by the Court. However, in the Apex Court through a five judge Bench, unanimously struck down Section 377 of the IPC to the extent that it criminalised the same -sex relations between two consenting adults. In doing so, it was declared that the State can't intrude into one's choice of partner, personal intimacy or love. The right to privacy is a fundamental right and the right to sexual orientation is an intrinsic part of that right[31].
- Selvi & Ors v. State of Karnataka[32], also serves as a crucial stepping point in the growth of privacy as a fundamental right. The Supreme Court here made a distinction between physical and mental privacy. The Court here decided that no individual should be forced

[28] AIR 1999 SC 495, (1998) 8 SCC 296
[29]District Registrar and Collector, Hyderabad v. Canara Bank (2005) 1 SCC 496, AIR 2005 SC 186

[30] CRI. L. J. 94, 2009 (6) SCC 712

[31] Navtej Singh Johar and Ors. vs. Union of India AIR 2018 SC 4321, (2018) 10 SCC 1

[32] AIR 2010 SC 1974, (2010) 7 SCC 263

to take any tests, such as narcotics or polygraph tests, against their own consent, as allowing that amounts to an intrusion into one's personal space and liberty.

- Internet Freedom Foundation v. Union of India (2019): Considered to be another landmark decision in the realm of the right to privacy, the case dealt with the issue of internet shutdowns and how they impact the right to privacy. The Supreme Court held that the suspension of internet services is against our fundamental rights and must not be permitted unless they adhere to the principles of necessity and proportionality.
- Unique Identification Authority of India v. Central Bureau of Investigation (2014): The court in this fascinating case decided on the issue of whether collection of biometrics by the UIDAI without the consent of the person violated the right to privacy. The court upheld the constitutionality of the Aadhar but also imposed certain restrictions on the data collection to allow people to safeguard their privacy. The decision assumes even more significance as it tries to maintain a delicate balance between the aim of the government with that of an individual's privacy rights.
- In a recent case of X v. The Principal Secretary, Health and Family Welfare Department, Govt. of NCT of Delhi & Anr.[33](2022), rendered by the Apex Court, the reproductive autonomy of an unmarried woman was upheld. As per the facts of the case, the Bench permitted a 25 year old woman to undergo abortion as her right to bodily autonomy is guaranteed in Article 21 of the Constitution. The right to privacy enables a person to exercise bodily autonomy under Article 21.
- In a case, more popularly titled as, the Hadiya marriage case[34], the Apex Court noted that an individual's right to marry a person of one's choice is a part of her privacy and that the state has no role and no power in interfering with the right. It was held that the right to privacy also includes an essential aspect of making decisions on close matters of one's life.
- The significance of the right to privacy can also be seen in the decision where the Apex Court decriminalised adultery mentioned in Section 497 of the IPC. Justice Chandrachud, writing the concurring opinion on the subject matter, stated that Section 497 criminalises adultery that was put in place to reinforce the idea that in marriage, a woman loses her autonomy and agency. She loses her own identity and is restricted to

[33] 2022 SCC OnLine SC 1321
[34] Shafin Jahan vs. Asokan K.M. and Ors (2018) 16 SCC 368, AIR 2018 SC 1933

the patriarchal norms of society. J. Chandrachud employed the concept of right to privacy in deciding to decriminalise adultery as an offence[35].

- Even though in most of the cases, courts didn't explicitly recognise the right to privacy, the highest court of the country ruled in favour of the existence of the right in the landmark decision of K.S. Puttaswamy v. Union of India[36].The decision delivered in 2018 by a 9 judge bench read the right to privacy within the ambit of Article 21, which is the right to life and liberty. In declaring that the right to privacy is intrinsic to life and personal liberty, the Court overruled earlier decisions of MP Sharma and Kharak Singh that held that privacy wasn't protected as per the Indian constitution. The Bench declared the following in the decision:

1. The recognition of the right to privacy in no way means amending the Constitution or granting a new freedom; it is just the interpretation of already existing provisions.
2. Privacy aims to protect personal intimacies, sanctity of personal life, marriage, reproduction, sexual orientation, etc.
3. Privacy also means the right to be left alone.
4. Just because a person sets out his foot in a public place doesn't mean he surrenders all his rights to privacy. It is attached to a person, no matter where he is or goes.
5. The Constitution must be interpreted liberally to allow growth and development with technological changes.
6. However, even though the right to privacy is a basic right, it's not an absolute right. Like every other fundamental right, it also has a set of reasonable restrictions imposed upon its usage.
7. Privacy has both positive and negative connotations. The negative part restricts the state from doing any act that may violate an individual's right to privacy and the positive connotation denotes the proactive duty imposed on the state to protect the right to privacy.
8. The recognition of the right to privacy as a fundamental right protects the inner sphere of an individual from interference by state and non-state actors.
9. The right to privacy can't be denied, even if there's a tiny fraction of people who are affected by it.

[35] Joseph Shine vs. Union of India (2019) 3 SCC 39, AIR 2018 SC 4898

[36] (2019) 1 SCC 1

CONCLUSION

The evolution of data protection in India reflects a growing recognition of the importance of privacy in digital age. From a backdrop of minimal regulation, the country is gradually formulating a more robust framework aimed at protecting personal information, balancing individual rights with economic and technological growth.