THE RIGHT TO PRIVACY IN INDIA: EVOLUTION, SCOPE AND CONTEMPORARY CHALLENGES

Maher Dave, KES Shri Jayantilal H. Patel Law College

ABSTRACT

The right to privacy has been under scrutiny in India for many years and has now emerged as a cornerstone of modern constitutional democracy. Today, it is rightfully considered one of the most important fundamental rights. Over the years, the idea of privacy has been debated in the courts, and it gained recognition after the landmark Supreme Court judgment in *Justice K.S. Puttaswamy v. Union of India (2017)*. There have been many instances in the past that created a need to discuss this right and lay down certain rules or guidelines to define its scope and applicability. Each time, the issues raised were different, but the core issue remained the same. This issue has gained greater attention today due to the rapid growth of digital technologies, data-driven governance, and social media platforms such as Facebook, Instagram, WhatsApp and Twitter. Nowadays, citizens all over the world generate a lot of digital footprints through social media platforms and also through mobile phones and the internet. This personal data is highly vulnerable to misuse and unauthorised access. Respecting this right is essential to personal liberty.

This research paper analyses a wide array of issues concerning informational privacy in India, and examines how constitutional jurisprudence has moulded the right to privacy in the country. It discusses the pre-independence era, the Universal Declaration of Human Rights (1948), and the reform of law through landmark Supreme Court cases such as Puttaswamy v. Union of India, *M.P. Sharma v. Satish Chandra (1954),* and *Kharak Singh v. State of Uttar Pradesh* (1962). This paper also examines the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023.

The paper even scrutinises contemporary issues, such as phone tapping, data leaks, cybercrime and the alleged leak of WhatsApp chats related to the Sushant Singh Rajput suicide case. A brief comparison with the General Data Protection Regulation of the European Union is also provided. This paper concludes by suggesting necessary reforms to strengthen data protection and balance innovation and technological development in India.

Keywords: Constitutional Democracy, social media, Supreme Court cases, Sushant Singh Rajput, European Union, Data protection, Information Technology Act, 2000

Introduction

Privacy is considered a fundamental human right that enables an individual to maintain control over personal information and life. Privacy is not restricted just to social media platforms, digital banking systems and other online platforms; it is also applicable to physical spaces, such as houses and personal correspondence. Consequently, the concept of informational privacy has become more and more important in recent times.

It is essential for legal systems to keep pace with technological developments in order to adequately protect individual rights. Several amendments to existing statutes, along with the development and enactment of new statutes, have helped the Indian legal system evolve into a robust framework for protecting people's rights. Privacy can take various forms, including data privacy, spatial privacy, communication privacy, bodily privacy, intellectual privacy, psychological privacy and anonymity.

The Universal Declaration of Human Rights (UDHR), through Article 12, articulates the right to privacy as follows:

"No one shall be subjected to arbitrary interference with their privacy, home, family or correspondence, nor to attack upon their honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

A major turning point came in 2017 when the Supreme Court delivered its historic judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India*. A bench of nine judges unanimously declared that privacy is a fundamental right protected under Articles 14, 19 and 21 of the Constitution. The court also held that it is intrinsic to life and personal liberty. The concurring opinions of the judges strengthened the right to privacy by recognising personal decisions, such as food consumption and bodily integrity (e.g., reproductive rights), and the protection of personal information, such as the privacy of health records. This judgment marked a major shift in Indian Constitutional law and laid the foundation for the modern data protection legislation.

Today, the right to privacy plays a crucial role in addressing issues such as cybercrime, misuse of personal information, data breaches and government surveillance. Therefore, the right to privacy as a fundamental right has created new legal responsibilities for both the State and

private entities.

Pre-Independence and International Recognition of Privacy

In India, the right to privacy was formally recognised much later, even though the concept existed long before independence. Earlier legal frameworks were primarily designed to maintain order rather than to protect individual liberties. According to Black's Law Dictionary, the word 'privacy' means the "right to be let alone", which indicates that a person should be free from any unwarranted intrusion or publicity. The concept of privacy is broad and may vary from person to person.

The theory of privacy has a historical background. It can be traced back to ancient Indian texts such as the Mahabharata and the Ramayana. These scriptures contained norms regarding privacy that people followed. They reflect social norms that emphasise respect for personal boundaries. They prohibited a man from watching a sleeping woman, naked women or taking her alone to someone's house without permission. Kautilya's Arthashastra has a reference to the word Avarana (आवरण), meaning protection or concealment. It was meant to protect the privacy of women. Kautilya had also emphasised the importance of confidentiality in state affairs, particularly during discussions among ministers.

The idea of respecting personal space and avoiding intrusion into private life has been recognised across different cultures and traditions in India. These examples indicate that the concept of privacy has long been present in social and cultural practices.

International developments have also played an important role in shaping modern privacy laws. There are 3 International instruments to safeguard privacy:

- Article 12 of the Universal Declaration of Human Rights
- The International Covenant on Civil and Political Rights (1966)
- The European Convention on Human Rights and Fundamental Freedoms (1950)

The Universal Declaration of Human Rights is considered one of the most important instruments, as stated in Article 12 of the Constitution. Article 12 includes various components such as:

- Family Privacy
- Individual Privacy
- Correspondence Privacy
- Privacy related to honour and reputation

Major importance is given to individual privacy under this Article because it protects the person's dignity and personal liberty. The right against arbitrary interference or attack is given specific protection. There are two types of laws:

- Common laws - Countries like the U.K., U.S.A., Canada, India, Australia and South Africa follow common laws.
- Civil laws - Countries like Germany, France and China follow civil law

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) protects people against arbitrary interference with their privacy. India ratified the ICCPR on April 10, 1979, without reservations. This provision has significantly influenced the recognition of privacy rights in India.

Evolution of Privacy Jurisprudence in India

The development of privacy can be understood through key judgments of the Supreme Court:

M.P. Sharma v. Satish Chandra

In M.P. Sharma v. Satish Chandra, the investigation alleged into financial irregularities in a company called Dalmia Jain Group. The company had gone into liquidation in 1952 after the Government of India ordered an investigation under the Companies Act, 1913. An investigation was conducted and it was revealed that the company attempted to embezzle funds by falsifying balance sheets and accounts. A FIR was registered and search of the premise was conducted following an order by the District Magistrate. The main issue which arose was that whether such practice of search and seizure of documents caused infringement of the Indian Constitution.

The case was heard by an eight-judge bench of the Supreme Court in the year 1954 to determine whether search and seizure violated fundamental rights. The judgment stated that right to privacy was not a fundamental right under the constitution of India at that time. Article 20(3) uses the term such as "to be a witness" which protects against the compelled testimony as it did not simply apply to verbal testimony but would include the production of documents.

Kharak Singh v. State of Uttar Pradesh

The right to privacy issue had emerged again before the judiciary in 1962 in Kharak Singh case. He was suspected of being involved in a dacoity case. There was a lack of evidence against him but U.P. Police opened a charge history under chapter 20 of the UP Police regulation. It involved secret picketing of petitioners' house, periodic inquires by officers, nightly domiciliary visits as well as tracking of his movements. He filed a writ petition under article 32 for challenging the constitutional validity of regulation 236 of UP Police regulations. The main issue was whether police, particularly visiting domiciliary at night, violated the fundamental rights of the petitioner, or such acts infringed the right to privacy. The six-judge bench was held which granted the Right to Privacy for the first time in Supreme Court of India but did not acknowledge it as a fundamental right. The Supreme Court delivered a majority decision partially in favour of the petitioner as they disturbed the personal liberty of an individual and violated Article 21 of the Constitution. The decision also emphasised the need of privacy and importance of procedural safeguards rather than subjective satisfaction.

This led to the establishment of principle that the right to privacy is a fundamental right and should be restricted only through procedures established by law.

Constitutional Recognition of Privacy

If we look at the preamble, the dignity of an individual is already assured, and it has been observed and discussed that privacy is an integral part of human dignity. Therefore, it has laid the ground for the development and incorporation of the right to privacy in the Indian Constitution. The enforcement of this right is ensured through constitutional remedies under Articles 32 and 226.

Justice K. S. Puttaswamy (Retd.) v. Union of India and Ors.

The petition was filed by Justice K.S. Puttaswamy (Retd.) against the Union of India before a

bench of nine judges of the Supreme Court. Then, a bench was set up to determine whether the Right to privacy was granted as a fundamental right by the Supreme Court. The court challenged the Aadhar scheme introduced by the Government of India which had made Aadhar number mandatory to access Government services, documents and benefits. This scheme required citizens to provide demographic and biometric information such as fingerprints and iris scans to receive the unique identification number. This was challenged before a three-judge bench as it violated the right to privacy of every citizen. The arguments made by the Attorney General were based on judgments of M.P. Sharma v. Satish Chandra (bench of eight judges) and Kharak Singh v. State of Uttar Pradesh (bench of six judges). This also formed the basis of later decisions for smaller benches of Supreme Court which recognised the Right to Privacy.

The petitioner argued before the nine-judge bench that this right was an independent right which guaranteed the right to life with dignity under Article 21 of the Constitution. He said the nature of fundamental rights was theoretical and philosophical as it contained detailed arguments of constitutional interpretation. The main issue was whether the right to privacy was a fundamental right under Part III of the Constitution of India.

Bench of nine judges unanimously upheld that the right to privacy is a constitutional right. The right to privacy was reinforced by the opinion of the judges in this case. This right includes autonomy over personal decisions (e.g. consumption of beef and alcohol), bodily integrity (e.g. reproductive rights) and protection of personal information (e.g. privacy of health rights). The law provides for data protection and regulates National Security, which allows interception of data by the state. The reasonable restrictions on privacy were imposed by the state and it had three conditions such as:

- Legality - There must be a law authorizing the action
- Legitimate State Aim - The action must pursue a legitimate public purpose
- Proportionality - The interference must be proportionate and necessary

Hon'ble Justice Shri B.N. Srikrishna had drafted the Data Protection Bill, 2019, which was reviewed by a joint committee of Parliament that submitted its final recommendations and a revised draft bill in November, 2021.

Puttaswamy case is a landmark in various aspects as it ends the controversy of privacy and

declares it as a part of the Right to Life Personal Liberty under Article 21 as fundamental right guaranteed by Part III of the Constitution. In the digital age, individuals often share personal data for various purposes, making the protection of privacy increasingly important. This judgment remains a cornerstone of privacy jurisprudence in India.

Informational privacy in the digital era

Informational privacy refers to an individual's ability to control personal information. Internet connectivity, hardware and software have become increasingly integral to daily life, and the challenges related to privacy have grown manifold. In the digital era, privacy encompasses multiple dimensions such as communication privacy, informational privacy and individual privacy. Each of them is unique. Informational privacy deals with the protection of personal data collected by entities, and on the other side, communication privacy deals with the unauthorised use and distribution of personal communications. Individual privacy pertains to the protection of one's identity online. Day-to-day activities have become intertwined with digital platforms, making people's date vulnerable to misuse.

Personal information of people has become an asset for many businesses because it allows them to better understand and target consumers. Any unauthorised and unregulated use of such information can lead to problems for individuals, including identity theft, financial fraud and indiscriminate surveillance. Governments have their reason for collecting data for issues such as national security and crime prevention, but without proper regulation, it can lead to infringement on civil liberties.

The Information Technology Act, 2000 (popularly known as The IT Act) was enacted by the Indian Parliament and received Presidential assent on 9 June 2000. It became effective from 17 October 2000. It was influenced by the UNCITRAL Model Law on Electronic Commerce and forms the foundation of cyber law in India. The Act has been supplemented by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. It contains several key features:

- Legal recognition of electronic signatures, ensuring that digital transactions and contracts are legally valid like handwritten signatures.
- If any person accesses or secures access to a device or computer system, then it

establishes criminal liability.

- Provision of prosecution for several cybercrimes such as identity theft, hacking, cyber terrorism and cyber stalking. It also provides legal recourse for victims of cybercrimes.
- Creation of a hierarchy of regulatory bodies, including the adjudicating officers for cyber regulation.
- Intermediary guidelines and Digital Media Ethics Code Rules of 2021, which helped the Information Technology Act to introduce a framework to regulate social media platforms and digital news content, measuring objectionable content and user data privacy.
- Certain devices may be designated as secure under the Act.

The Act has undergone several amendments to address emerging forms of cybercrime. Section 66A, which dealt with offensive online content, was struck down by the Supreme Court in *Shreya Singhal v. Union of India* as unconstitutional. Section 72A imposes penalties for disclosure of personal information in breach of lawful contracts.

Even after amendments in the IT Act, India still lacks a real data security and privacy legislative system. There are threats to privacy on the internet, such as:

- The information gathered by cookies is sold to third parties.
- Use of cookies, trojans, web bugs and other viruses to collect personal information.
- Cookies enable a website to recognise the person and remember their preferences.
- Advertisers deploy trackers to track user preferences.
- A web bug enables a third party to monitor the person who reads a web page or an email message.

Therefore, the IT Act serves as the foundation for cyber laws in India. It adapts to the growing digital landscape, regulates electronic transactions, ensures tackling of cyber-crimes, establishes legal recognition and ensures security of digital transactions. It also plays an

important role in safeguarding the interests of individuals, businesses and Governments in the digital space.

Social media has earned a strong status in the digital era. It also has a considerable impact on personal privacy with its unique complexities and challenges. Social media is an easy target for invasion of privacy, such as cyber stalking, identity theft or invasive targeted advertising. In modern digital societies, individuals constantly expose their personal information through:

- Mobile phones
- Online Shopping
- Digital banking system
- Internet browsing

Privacy settings on social media platforms also play a major role in user privacy by controlling user content and information that is publicly accessible. Some social media platforms have faced criticism for sharing user data with third parties without explicit consent. Policies and practices of each platform must provide users with more control over their digital privacy.

The relationship between social media and privacy is intricate and complex. It has its own advantages and disadvantages. Social media requires a balance between potential risk and exercising caution with the information shared. Therefore, strong data protection laws are required in the country.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 is a landmark legislation enacted by the Parliament of India to protect personal data in the digital environment. The Act was passed by both Houses of Parliament in August 2023 and received Presidential assent on 11 August 2023. It forms an important part of India's privacy framework, especially after the recognition of privacy as a fundamental right by the Supreme Court in *Justice K.S. Puttaswamy v. Union of India*.

The Act aims to protect individuals' right to privacy. It allows lawful use of personal data for legitimate purposes. It represents India's first comprehensive legal framework dedicated to

digital personal data protection.

The Act applies to processing digital personal data, which refers to any information relating to an identifiable individual processed in digital form. Personal data includes details such as contact number, email address, person's name, identification number, biometric or online identifiers. It also seeks to regulate data that is stored, used and shared by the organisation to protect individual privacy in the digital environment. The Act applies not only to data collected digitally through various means, such as websites, mobile applications or online services, but also to data that is collected in offline form and later converted into digital format. For example, if a company collects personal information through a physical form and later stores it in a digital database, the provisions of the act will also apply to such cases. The act also has some exceptions to its applicability.

This act also has an extraterritorial application, which means that the provisions of the law apply not only to organisations operating within India but also to foreign entities handling the personal data of individuals in India.

Despite its significance, the Act has been criticised on several grounds:

- The bill does not fully address risks of harm arising from the processing of personal data.

- The bill allows transfer of personal data outside India, except to countries notified by the Central Government. This mechanism may not ensure adequate evaluation of data protection standards in countries where the transfer of data is allowed.

- The members of the Data Protection Board of India are appointed for two years and will be eligible for re-appointment. This may affect the independent functioning of the Board.

- Exemptions to data processing by the state on grounds such as national security may lead to data collection, processing and retention beyond the required purpose. This may violate the fundamental right to privacy.

The act grants certain rights to individuals, including the right to obtain information, seek corrections and get redressal of grievances. The Central Government may exempt government

agencies from the application of provisions of the bill in the interest of specified grounds such as security of the state, public order and prevention of offences. Personal data may be processed only for a lawful purpose with the consent of an individual. Consent may not be required for specified legitimate uses such as voluntary sharing of data by an individual or processing by the state for permits, licenses, benefits and services.

Data fiduciaries will be obligated to maintain the accuracy and security of data and delete it once its purpose has been served. The Digital Personal Data Protection Act also includes several important legal concepts such as Data Principal, Data Fiduciary and Data Processor. It defines the roles and responsibilities of various participants involved in the collection and management of personal data. It helps to establish a structured framework for regulating data practices in the digital world.

One of the most important terms in this Act is 'Data Principal'. It relates to the collection and processing of people's personal information. The act grants them rights and certain protection, such as the right to access their data, the right to correct inaccurate information and the right to withdraw consent for data processing. For example, if a person provides his personal data, such as email address or phone number, while using an online service, then that person becomes a Data Principal.

Another key concept in this Act is of 'Data Fiduciary'. It means any individual, company, government official or organisation that determines the purpose of processing personal data. It has several responsibilities, such as obtaining the consent of the Data Principal before collecting data, implementing security safeguards to protect the data from misuse and ensuring its use only for legitimate purposes. For example, the collection of biometric and demographic data under governmental schemes like Aadhaar.

The Act also recognises the role of Data Processors. The Data Processor is an entity that processes personal data on behalf of the Data Fiduciary. It processes the data according to the instructions given by the Data Fiduciary and does not devise the purpose of data collection. For example, a technology service provider that manages data storage or analyses data for the company may act as a Data Processor.

Data Protection Board of India

It is an important regulatory authority established under the Digital Personal Data Protection

Act. It came into effect from 13 November 2025. The main objective of this board is to ensure proper implementation of the provisions of the act and protection of personal data of individuals from misuse.

The Board has been vested with the power to issue binding directions to secure compliance, exercise civil court powers like issuing summons, evidence and conducting an inspection to ascertain facts and impose monetary penalties in cases of non-compliance. The Board does not appear to be empowered to award special damages, but rather to deal with regulatory complaints and breach cases.

This act repeals section 43A of the Information Technology Act, 2000, which provided a specific statutory compensation mechanism to protect personal data. For example, if a digital company leaks personal information without consent, it may affect the individual, and they can approach the Data Protection Board, which may investigate the matter and impose penalties on the company.

The Board is the central regulatory authority of the framework. It is empowered to initiate inquiries, issue directions and impose significant monetary penalties.

Cyber Protection Laws and Surveillance Issues

There has been a rapid growth in digital technology and internet connectivity, which has increased concerns regarding the protection of personal data and informational privacy. Digital platforms such as online transactions, banking and social media networking have created chances for cyber criminals and unauthorised actors to exploit personal data.

Cybercrimes include activities such as phishing, online fraud, hacking, unauthorised access to computer systems and identity theft. Such acts lead to violation of an individual's informational privacy and may result in reputational damage, financial loss and misuse of data. The Information Technology Act was introduced to provide legal provisions to deal with cyber offences and protect electronic data. State Surveillance is also a major concern in the digital world, particularly the interception and monitoring of private communications. With the advancement of technology, governments possess powerful tools that enable them to monitor phone calls, email addresses and online activities. Surveillance is necessary to maintain national security, prevent crime and protect public order, as it can infringe upon an individual's

right to privacy.

One of the most controversial forms of surveillance is phone tapping, which means the interception of telephone conversations without the knowledge of the concerned individuals. Under Indian law, interception is allowed only under specific conditions such as threats to national security, prevention of serious crimes and public safety.

People's Union for Civil Liberties v. Union of India

The Supreme Court addressed the issue of telephone interception in the landmark *People's Union for Civil Liberties v. Union of India* case. This case was examined to check whether the Government's power to intercept the telephone conversations under the Indian Telegraph Act violated the fundamental rights of the citizens guaranteed under Article 21 of the Constitution.

The case was filed by a civil rights organisation, People's Union for Civil Liberties after reports appeared in newspapers about widespread telephone taping by government officials. The petition challenged the constitutional validity of Section 5(2) of the Indian Telegraph Act, which allowed the government to intercept communications on specified grounds, including sovereignty and integrity of India. The petitioner claimed that the government violated an individual's right to privacy.

The primary issue before the Supreme Court was:

- Whether Section 5(2) of the Act was used to infringe the right to privacy,
- Whether there was a need to read down Section 5(2) of the Act to include Procedural safeguards to preclude arbitrariness and prevent indiscriminate phone tapping.

The court observed that the right to have a telephonic conversation in the privacy of one's own home or office without interference can be claimed as a right to privacy. It also held that the telephone tapping would violate Article 21 of the Constitution unless it was permitted under a procedure established by law. The court also stated that telephone conversations were an exercise of a citizen's right to freedom of speech and expression under Article 19(1)(a), and any restriction under Article 19(2) of the Constitution must be reasonable. Besides, it observed that telephone tapping is a serious invasion of privacy. The Court recognised that interception may be permitted under Section 5(2) on limited grounds such as -

1. Sovereignty and Integrity of India
2. Security of the State
3. Friendly relations with the foreign states
4. Public order
5. Prevention of incitement to the commission of an offence

The court did not completely prohibit phone tapping but emphasised that it must be carried out only under strict legal procedures and safeguards. To prevent misuse of surveillance powers, it laid down several important guidelines:

- Orders for phone tapping could be issued by the Home Secretary of the State Government, or the Central Government, and the power can only be delegated in an emergency.
- Review Committee should be constituted at the Central and State levels to assess compliance with the law.
- Detailed records of the intercepted communication were to be maintained.
- The authority making the interception order must consider whether it was necessary to obtain the information through such orders.
- The use of intercepted materials was limited, and the intercepted material would be destroyed when retention became unnecessary.
- The interception order would cease to be effective two months after the date of issue and limit the total period of the operation of the order to six months.

Contemporary Privacy Concerns

In the modern era, there is technological advancement and widespread use of the internet, which have created complex challenges for the protection of individual privacy. There is an increase in large-scale collection and storage of personal data through social media platforms, cloud storage and digital communication tools. These technologies have improved communication and access to information, but also have some drawbacks, such as increased

risk of unauthorised access, data breaches and misuse of personal data. Concerns relating to informational privacy have become more serious in contemporary society.

The death of the Bollywood actor Sushant Singh Rajput in 2020 was a case of controversy related to privacy. During investigations, it was discovered that several private WhatsApp messages that belonged to the actor were leaked to the media. Public debate and speculation had arisen regarding his death because of the leaks on television channels and social media platforms. Even though WhatsApp uses encryption to protect users' data and private information, it may still be exposed when accessed by investigators or other parties without proper safeguards. This raises serious concerns about the sensitivity of the data handled during criminal investigations. The incident also highlighted the tension between freedom of the press and the right to privacy. The publication of private communications may violate an individual's dignity and personal autonomy, and demonstrates the need for stricter rules governing digital evidence and data protection. The broadcasting of personal chats raised ethical questions about whether media organisations should publish private information that may not be directly relevant to the investigation. When private messages are leaked to the public, it can lead to reputational harm, emotional distress and misinformation for the individuals involved. The personal data obtained during investigations has to be handled responsibly and kept confidential. The case sparked a debate regarding the responsibility of law and media organisations in safeguarding personal information obtained during investigations. It also highlights the growing challenges to privacy in the digital age and involves criminal investigations. It demonstrates the urgent need to balance transparency, protection of individuals' private information and freedom of the press.

Tracking technologies present significant challenges to digital privacy. The dynamic nature of these digital risks makes it challenging to provide complete safeguards. Individuals must remain vigilant and informed about the risks associated with sharing personal data. Privacy remains a fundamental right even in an increasingly digital society. In the digital age, we need to maintain and respect digital privacy as it challenges the necessity for constant vigilance, robust cybersecurity and ongoing education. Privacy remains a fundamental human right even as humans navigate this increasingly digital world.

Privacy within the home

Privacy is not limited to personal information or digital data, but it also extends to the protection

of an individual's life within the home. Home is defined as the most secure and personal space where an individual can perform his own tasks and can move freely without interference from the State or any other person. Article 21 of the Constitution of India is linked with the protection of privacy within the home, and even the right to life and personal liberty is secured. The Constitution seeks to safeguard the dignity and autonomy of an individual, i.e. protecting individuals against arbitrary intrusion into their homes.

Any unauthorised entry or surveillance within a person's residence can amount to a violation of privacy. Surveillance also includes monitoring activities or installing devices within private residences to observe individuals without lawful permission, which may constitute an unjustified intrusion into personal life. For example, when an illegal search is conducted without proper legal authorisation, such as warrants issued by a competent authority, it may infringe upon an individual's private life.

Various forms of violation may occur, and one such form is violation through recording or interception of private conversations within the home. In a residence, various discussions take place that are expected to remain confidential, or disclosure of such discussions can undermine the trust and security associated with personal living spaces.

The Supreme Court has affirmed that privacy is an intrinsic part of the right to life after the *Justice K.S. Puttaswamy v. Union of India* case.

The concept of privacy within the home is a broader concept which involves that every individual is entitled to personal space where personal relationships, daily activities and family life take place without unlawful intrusion. It is essential to protect this sphere of privacy because it maintains human dignity, personal freedom and the sanctity of individual life in a democratic society.

General Data Protection Regulation

The General Data Protection Regulation is commonly known as GDPR. It is one of the most stringent privacy laws in the world. GDPR is one of the most comprehensive and stringent data protection frameworks in the world. It was adopted by the European Union in 2016 and came into effect in 2018. The main aim of GDPR is to strengthen the protection of personal data and ensure that individuals have control over how their personal data is collected, stored and

processed by organisations. The GDPR levies hefty fines on those who violate the privacy and security standards. It is also defined as a legally approved way to transfer and process personal data, detailing how organisations must protect personal data at rest and in transit. It sets several principles that controllers and processors must follow while handling personal data. The processing activities must be clearly defined, transparent and fair.

GDPR Requirements:

Data protection assessment

The regulation requires organisations to conduct a Data Protection Impact Assessment where data processing activities pose significant risks. Certain organisations must appoint a Data Protection Officer to oversee compliance.

The GDPR also regulates the transfer of data to third parties and requires safeguards to ensure adequate protection. In the event of a data breach, organisations must notify authorities and, in some cases, affected individuals.

The GDPR grants several rights to individuals, including the right to be informed, access personal data, seek correction, request erasure, and transfer data. It also protects automated decision-making. Additional safeguards are provided for sensitive personal data, such as health or biometric information.

Data protection officers

Certain organisations must appoint a Data Protection Officer (DPO) to oversee compliance with GDPR. A DPO has various responsibilities such as advising organisations on GDPR, data protection law, overseeing data protection impact assessment and acting as the government regulators. Companies must appoint a DPO if they monitor on a large scale or process special category data as a core activity.

Data transfer safeguard and procedures

Data controllers are responsible for any data they share with a third party. Controllers and processors often enter into formal data processing agreements to comply with GDPR. They bind contract outline details like the kind of processing a processor and the type of security

they must employ. The controller's data cannot be used by the third party for their personal use.

Data breach notification

If there is any breach of data, then the controller must report it to a supervisory authority within 72 hours. A breach can pose a risk to data subjects, such as monetary or identity theft. The company must notify them. Breach notifications are sent directly to the victims, which include details about the kind of data stolen, risks to subjects and how the company is addressing the issue. Notification is not required if the data is heavily encrypted and unusable to hackers.

The General Data Protection Regulation grants extensive rights to individuals, often known as 'Data Subjects'. There are various rights, such as:

- Right to be informed about data collection and processing: Data subjects have the right to know who has access to data, how they got it and what they are doing with it.
- Right of access: The right to access any data that a company has is with the data subject
- Right to rectification: Data subjects also have the right to correct inaccurate or outdated personal data.
- Right to erasure: Companies must comply with their interest in the data (e.g. legal obligation to maintain certain records)
- Right to restriction of possessing: If the data is inaccurate or no longer necessary for the company's purpose, then the company may ask to limit how its data is used.
- Right to data portability: The subjects have the right to move data from one company to another. There are various data that can be transferred to a third party at the subject's request.
- Right to object: The company must stop processing if it proves to be legitimate.
- Right related to automated decision making and profiling: Significant decisions cannot be made without the consent of people. They can offer input on the decision and demand that the company review the decision.

GDPR also considers some sensitive data. There are special categories that include information on a person's race or ethnicity, religious beliefs, biometric data and political opinion, among other things. Special category data can only be processed by the company under very specific circumstances. They are not limited to:

- Subject granted explicit consent
- Processing is necessary for scientific research
- Data on criminal convictions can only be controlled by official authorities and processed in their direction.

Organisations are required to implement strong security measures and maintain accountability in data processing. Non-compliance with the GDPR may result in significant financial penalties.

Criticisms

Even though the GDPR is a strong mechanism, it has faced criticism. Compliance requirements may result in administrative and financial stresses, particularly on small and medium enterprises. The framework is very complex and it may be difficult to implement it effectively. Some critics are of the opinion that strict data protection rules may affect innovation, particularly in fields such as artificial intelligence and data analytics. At the same time, restrictions over cross-border data transfers may create practical challenges for global businesses.

Conclusion

The right to privacy has now been unarguably recognised as a fundamental right. This acceptance is a milestone in Indian constitutional law. In a rapidly changing and digitising society, it is very important to protect personal data. In view of this, legislative measures such as the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023, are significant steps in this direction.

The idea of protecting privacy has evolved over several decades. At one point, it was meant to safeguard individuals from state interference, but its scope has now widened to cover intrusion

by private entities, particularly in the digital space. It is now beyond doubt that the right to privacy is an integral part of the right to life and personal liberty under Article 21 of the Constitution.

It was the landmark judgment in *Justice K.S. Puttaswamy v. Union of India* that has played a crucial role in recognising informational privacy as a core element of this right. It led to the enactment of data protection legislation. However, the current framework has been criticised for certain breaches and inadequacies.

To empower citizens to better protect their data, public awareness and digital literacy are essential. India needs to take multi-pronged steps, including strengthening regulatory institutions such as the Data Protection Board, to ensure effective enforcement and grievance redressal. Privacy rights are not supposed to be theoretical. Strong mechanisms for their enforcement, as well as accountability for organisations handling personal data, must be established.

While India supports innovation and digital growth, it must ensure the effective protection of individual privacy.

References

1. GeeksforGeeks, S. (2026, March 26). Information technology act, 2000 (IT act). https://www.geeksforgeeks.org/ethical-hacking/information-technology-act-2000-india/

2. Research, P. (2026, April 7). The Digital Personal Data Protection bill, 2023. PRS Legislative Research. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

3. Banerji, O. (2024, February 5). Right to privacy. iPleaders. https://blog.ipleaders.in/different-aspects-of-right-to-privacy-under-article-21/

4. Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (n.d.). https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors

5. Editor, V. (2026, January 6). Right to privacy, evolution, significance, challenges. Vajiram and Ravi. https://vajiramandravi.com/upsc-exam/right-to-privacy/

6. The Digital Personal Data Protection Bill, 2023. (n.d.-b). PRS Legislative Research. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

7. Piper, D. (2024). Data Protection in India. Data protection laws in India - Data Protection Laws of the World. https://www.dlapiperdataprotection.com/?t=law&c=IN

8. Cybersecurity Law: Protecting Data in the Digital Age | Avantika University. (n.d.). https://www.avantikauniversity.edu.in/blog/cybersecurity-law-protecting-data-in-the-digital-age

9. PUCL v. Union of India: The NOTA CASE 2013. (n.d.). ALEC - Aashayein Law Education Center. https://www.alec.co.in/judgement-page/pucl-v-union-of-india-the-nota-case-2013

10. Centre for communication governance. (n.d.-a). Year. People's Union for Civil Liberties vs. Union of India & Ors. https://privacylibrary.ccgnlud.org/case/pucl-vs-union-of-india

11. KVN, R. (2020a). Sushant Singh rajput's death case: WhatsApp gives clarification on NCB team retrieving chat conversation. Deccan Herald. https://www.deccanherald.com/specials/sushant-singh-rajputs-death-case-whatsapp-gives-clarification-on-ncb-team-retrieving-chat-conversation-892824.html#

12. Pattnaik, N. (2023). A survey of User Perspectives on Security and privacy in ... ACM digital library. https://dl.acm.org/doi/pdf/10.1145/3558095

13. Cloudflare, C. (n.d.). What is the General Data Protection Regulation (GDPR)? | cloudflare. Cloudflare GDPR page. https://www.cloudflare.com/en-in/learning/privacy/what-is-the-gdpr/

14. Asthana, S., & Asthana, S. (2024, July 29). Article 21 of the Indian Constitution: Right to life and personal liberty. iPleaders. https://blog.ipleaders.in/article-21/

15. Apoorva, A. (2026, April 8). A background to Section 66A of the IT Act, 2000. PRS Legislative Research. https://prsindia.org/theprsblog/a-background-to-section-66a-of-the-it-act-2000?page=2&per-page=1

16. United Nations General Assembly. (n.d.). Universal declaration of human rights. United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights

17. Kalra, V. (n.d.). 1 an armistice between right to privacy and right of surveillance. http://docs.manupatra.in/newsline/articles/Upload/EA95AF38-5DF9-4211-B67A-36642B8F4464.1-A__Civil.pdf

18. Privacy in India: From Arthashastra to Digital Age • Philosophy Institute. Philosophy Institute. (2026, April 14). https://philosophy.institute/social-political/privacy-india-arthashastra-digital-age/

19. Taylor, P. M. (n.d.). Article 17: Privacy, home, correspondence; honour and reputation - a commentary on the International Covenant on Civil and Political Rights. Cambridge Core. https://www.cambridge.org/core/books/abs/commentary-on-the-international-covenant-on-civil-and-political-rights/article-17-privacy-home-correspondence-honour-and-reputation/5C2A432BF74C4289A49281A9279DAE35

20. United Nations, (n.d.). International Covenant on Civil and Political Rights. OHCHR. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

21. Supreme Court of India. (n.d.). Browse judgments. Indian Kanoon. https://indiankanoon.org/browse/

22. Year. M.P. Sharma & Ors. vs. Satish Chandra and Ors. (n.d.). https://privacylibrary.ccgnlud.org/case/saroj-rani-vs-sudarshan-kumar-chadha

23. Section 66A in the information technology act, 2000. (n.d.). https://indiankanoon.org/doc/170483278/

24. Wolford, B. (2025, August 19). What is GDPR, the EU's new Data Protection Law? GDPR.eu. https://gdpr.eu/what-is-gdpr/

25. Chen, J. (2020). GDPR explained: Key rules for data protection in the EU. Investopedia.https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp

26. Fortra. (2017). What is the GDPR? everything you need to know | fortra. https://www.fortra.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection

27. Welcome to the Human Rights E-Course. United For Human Rights. (n.d.). https://www.humanrights.com/course/lesson/articles-19-25/read-article-21.html

28. Patil, Dr. D. Y. (2022, March 16). International perspective of right to privacy. Dr. D. Y. Patil Law College, Pimpri, Pune. https://law.dypvp.edu.in/Blogs/international-perspective-of-right-to-privacy

29. Sehgal, D. R. (2020, August 3). Scope of right to privacy for phone tapping. iPleaders. https://blog.ipleaders.in/scope-right-privacy-phone-tapping/

30. M.P. Sharma and Others v. Satish Chandra, AIR 1954 SC 300

31. Kharak Singh v. State of Uttar Pradesh, AIR 1962 SC 1295

32. Justice K.S. Puttaswamy (Retd.) and Anr. vs. Union of India and Ors. (2017), AIR 2017 SC 4161