



THE EVOLUTION OF PRIVACY AS A FUNDAMENTAL RIGHT IN INDIA

JUDICIAL LANDMARKS, CONSTITUTIONAL CHALLENGES, AND CONTEMPORARY ISSUES

¹Anjali, ²Sarvagya Sushil

¹4th year Law Student, ²4th year Law Student

¹School of Law

¹Christ (Deemed to be University, Lavasa, India

Abstract: Privacy has become an extremely important human right around the world, and in India, it has been established as a Fundamental Right under Article 21 of the Indian Constitution. The Right to Privacy is closely related to the protection of personal data, which is difficult to safeguard in the current technological and globalized world. Moreover, there are instances where the right to privacy has been violated by the government through discriminatory legislation as the legal protection of this right is weak.

The Right to Privacy was not considered a Fundamental Right initially in India. There was no particular law made for protecting the privacy and data of the people of this country. Over time, various accusations have been leveled against the government and private firms about violating privacy. All such matters were presented before the courts. These courts issued significant judgments, guidelines, and rulings regarding such matters.

It is also important to discuss the legal developments regarding the Right to Privacy and data protection in view of these developments so that one gets to know the areas in which the Indian legal system is doing well in safeguarding the right for citizens. Though the Indian legal framework has properly recognized the Right to Privacy and took suitable steps to prevent data theft and misuse of sensitive information, considerable progress still needs to be made. There is the need for increased efforts towards broadening the area of data protection so that this Right to Privacy is given enough protection in this modern world.

Keywords - Data protection, Personal information, sensitive information, confidentiality, public interest

I. INTRODUCTION

Whether a topic of debate or not, privacy has now become an issue which it never did before, this being after the judgment pronounced by the Supreme Court of India on August 24, 2017 in the case of Justice K. S. Puttaswamy v. Union of India relating to clarification on the nature and scope of Right to Privacy. In the sense that individuals and societies feel about 'privacy', its meaning is also different. It has been extensively litigated before courts across the world and developed over time. Various landmark judgments both international and domestic, like Roe, Griswold, Prince Albert, and Indian judgments like Rajagopal and PUCL, have helped define this ambiguous concept and made it clearer over time. Now, Right to Privacy incorporates several

strands that have all been carefully worked upon by judicial attempts to make it more accessible and implementable for everyone.

1.1 Nature of the Right to Privacy

It has been decades since the nature of the Right to Privacy was not very clear whether it was a statutory right, a constitutional right, or a fundamental right. In cases where its scope could not be defined and where it was to be determined if there was any violation, the courts would seek the help of international legal frameworks. No country, however, has a Right to Privacy as enshrined in the constitution or laws. Instead, it has developed through interpretation and case law.

Judicial interpretation has formed the backbone of the emergence of the Right to Privacy. Most courts around the world, in order to keep up with the changing face of society, have adopted a case-by-case judgment process. This will always be provisional-generally trial and error-and through these processes, an abstract concept for privacy assumes more concrete and actionable form. Similarly, the other rights-Right to Food, Right to a Clean Environment, and the Right to Health-emerged as a result of judicial interpretation and show how judicial bodies have played a significant role in the growth of human rights.

1.2 First footprints of right to privacy

The Right to Privacy was first brought under judicial scrutiny in the case of *M.P. Sharma v. Satish Chandra*. In this case, the issue was privacy under the search and seizure provision of the Criminal Procedure Code. Here, the petitioner alleged that a search performed at his residence without notice interfered with his private domain. An eight-judge bench of the Supreme Court reflected on the question whether, in such circumstances, the petitioner had a Right to Privacy. The court mentioned the 4th Amendment to the United States Constitution, where privacy is talked about in connection with search and seizure operations and admitted that such a right did exist. But the question before court was whether the doctrine of privacy could fall within the ambit of Article 20(3) of the Indian Constitution that protects the person against self-incrimination. The Right to Privacy was not in dispute and, thus, did not decide on the issue of a common law Right to Privacy.

Another landmark case under the Right to Privacy is *Kharak Singh v. State of Uttar Pradesh*. This was a case in which a man was acquitted for being charged with dacoity (banditry) but was not allowed to go scot-free by the police, who kept watch on him. Under Regulation 236 of the Uttar Pradesh Police Regulations, surprise visits were paid to his home. The question whether the Regulation 236(b) was violative of Article 21 of the Constitution, conferring the right to personal liberty, was brought before the seven-judge bench.

The seven-judge bench interpreted the term "personal liberty" under Article 21. It held police surveillance to be an infringement on this constitutional right. On the other hand, Right to Privacy could not be construed since it did not find a comparable place in the American Constitution as its 4th Amendment. Indian law Constitution The bench also drew strength from the judgment in *A.K. Gopalan v. State of Madras*, wherein it was held that

each and every fundamental right under the Indian Constitution is separate and cannot be extended or construed to incorporate the features of another right.

This gave rise to an incongruity: the judiciary admitted that police surveillance violated Article 21's right of personal liberty but refused to interpret Article 21 as including a Right to Privacy. This contradiction brought an urgent necessity for judicial declaration further to define the limits and nature of privacy as a fundamental right.

1.3 Drawing from foreign jurisprudence

The Right to Privacy was thereafter more clearly defined, following the pronouncement of *Gobind v. State of Madhya Pradesh* in 1975. In this case, the Supreme Court of India came to a juncture from which the trend of privacy law in India has been shaped further. One aspect of the decision was the consideration of foreign jurisprudence to define the contours of the Right to Privacy

in the Indian context, through landmark cases from the United States of America. The facts of *Gobind* were similar to *Kharak Singh v. State of Uttar Pradesh*, though the court gave a more comprehensive and progressive analysis.

1.4 Influence of U.S. Jurisprudence

1. *Griswold v. Connecticut* (1965)

In this case, the U.S. Supreme Court looked at a Connecticut law that made it a crime to use or give advice about birth control. The Court said that even though the U.S. Constitution doesn't directly mention a "right to privacy," this right is suggested (or implied) by several parts of the Constitution. The Court said that married couples have the right to privacy in their personal lives, including decisions about birth control. This decision helped establish the idea of privacy in the law.

2. *Roe v. Wade* (1973)

Here, the Supreme Court was asked if a woman has the right to have an abortion. The Court said that a woman's right to privacy includes the choice to end a pregnancy. However, the Court also said that the government can make rules about abortion to protect the woman's health. This case expanded the meaning of the right to privacy to include control over reproductive decisions.

Both these cases greatly impacted the Gobind bench.

Key Findings in Gobind

1.Right to Privacy

The privacy right is held to be an implied one with the protection available under Articles 19(1)(a) (right to freedom of speech and expression), 19(1)(d) (right to freedom of movement), and 21 (right to protection of life and personal liberty) of the Indian Constitution.

2.Not Absolute Right

He asserted that the Right to Privacy cannot be absolute because it is held subject to reasonable restrictions in the interest of public welfare and state security. As such, it is necessary for rights of privacy to be weighed upon case-to-case basis to equate individual liberty with state's interest.

1.5 International Precedents

The court in Gobind invoked Griswold and Roe, appropriating the novel idea of penumbral rights to create privacy under Indian constitutional law. The smaller benches of the Supreme Court continued this expansion of recognition of privacy in the following decisions:

1. PUCL v. Union of India (1997)

Telephone tapping was held to be violation of the Right to Privacy except for the circumstances covered by the law.

2. R. Rajagopal v. State of Tamil Nadu (1994)

This case defined the Right to Privacy as the "right to be let alone." This defined a framework with which the right to privacy could be balanced with the right to freedom of speech and expression under Article 19(1)(a).

These cases formed the bases of privacy jurisprudence in India, and culminated into the landmark Justice K.S. Puttaswamy v. Union of India (2017) judgment by the Supreme Court where it has categorically declared that the Right to Privacy is a fundamental right under Article 21, binding on all state actions.

1.6 Overlapping zones of fundamental rights

This led to the criticism that the decision in the case of Kharak Singh regarding the rejection of the Right to Privacy as an independent right was founded upon the binding opinion in the A.K. Gopalan case, which held that the fundamental rights were confined to certain provisions and that no new rights could be added or

overlap. That view, however, was overruled by an eleven-judge bench in *R.C. Cooper v. Union of India* and later by a seven-judge bench in *Maneka Gandhi v. Union of India*, which held that fundamental rights are not confined to fixed provisions, and overlapping of fundamental rights is valid and permissible.

1.7 Crystal clarity on the nature of right to privacy

The case of *Justice K. Puttaswamy v. Union of India*, decided on August 24, 2017, finally settled all doubts about the nature of the Right to Privacy. A 9-judge bench unanimously declared the Right to Privacy as a fundamental right. This landmark judgment is a milestone in India's constitutional history and is expected to significantly impact the lives of citizens.

It all started in 2015 with the petitions against the constitutional validity of the Aadhar programme which was to be used for making a biometric database of all the citizens. This programme was seen as violating the Right to Privacy because it was to collect personal details of individuals, raising concerns that data could be misused by the government.

This issue was brought before a three-judge bench that directed the question of the nature of the Right to Privacy to be placed for consideration by a five-judge bench which, at that time, formed a nine-judge bench to determine whether the earlier judgments in *M.P. Sharma* and *Kharak Singh* were correct whereby the right to privacy is not a part of the basic structure and whether the right to privacy is, indeed, a fundamental right.

The 9-judge bench, with a unanimous 9:0 verdict, overruled *M.P. Sharma* and *Kharak Singh*, declared the Right to Privacy a fundamental right.

1.8 Compliance with international obligations-

The *Gobind* case and subsequent cases were followed by the recent judgment in *K.S. Puttaswamy v. Union of India*, wherein India was held liable to respect its international commitments as provided for in Article 51 of the Constitution, Article 12 of the UDHR, and Article 17 of the ICCPR. The conventions that India has ratified all guarantee inalienable human rights, including the Right to Privacy, which cannot be taken away under any circumstances.

Some rights are inalienable, according to the court, and are gifted to each human being from birth and cannot be taken away. International conventions are usually applied in case domestic law is absent or not inconsistent with the law already in place. One of the landmark judgments is *Vishakha v. State of Rajasthan*, in which the provisions of CEDAW and ICCPR were referred to and, subsequently, laws against sexual harassment at the workplace were enacted.

In these cases, it was also held that the Right to Privacy falls within the much wider ambit of Article 21 of the Constitution that guarantees the Right to Life. This guarantee of life includes life with dignity and puts the Right to Privacy as an essential element of one's dignity and freedom.

1.9 What is the concept of data privacy?

Data privacy has emerged as an issue of paramount importance due to technological advancement that made it extremely easy to retrieve information from anywhere on earth. The modern technology that made information exchange relatively easy has, in turn, introduced the issue of informational or data privacy.

Information is being collected on a large scale both by the governments and private persons, such as social networking websites like Facebook and Instagram, banks, hospitals, and restaurants. This data set includes information on an individual's preferences, medical history, travel history, and other confidential information. For example, health care facilities maintain health-related details like allergies, weight, and blood group. In the present digital world, personal information often has more value than physical possessions, with studies indicating that its value is over \$1200 if it is combined with consumer behavior patterns. The unauthorized disclosure of such information represents an infringement of privacy that highlights the importance of data privacy as an aspect of the Right to Privacy.

The Unique Identification Authority of India's (UIDAI) Aadhar project is the world's largest data collection project, which includes biometric data like fingerprints and retina scans. It was supposed to end problems like poverty, hunger, and circulation of fake currency. But it has been attacked for not doing anything better in giving access to basic items, such as food through PDS. In Rajasthan, 33 lakh families are said to have faced problems accessing rations after PDS was linked with Aadhar.

II. CRITICISM

The plan is criticized because it invades private rights, with the Supreme Court considering a constitutionality case based on this feature.

1.10 Other legal traditions Data protection

In most countries, the concept and legal framework for data privacy are more developed and comprehensive than in India. Most countries around the world have accepted data privacy as an integral part of the right to privacy. Such countries have well-formulated laws and regulations to safeguard the public's rights in data, so that personal information is dealt with care and security.

Position in U.S.A-

In the United States, the structure for data privacy is divided into several legislations. Among them, the two important acts are Privacy Act of 1974 and Computer Matching and Privacy Act that protect the data of the federal government. However, these acts do not cover the data owned by the private sectors. Data protection regulation of the United States is defined for different sectors instead of having a single legislation that is all-

inclusive. They encourage industries to regulate themselves, but when self-regulation does not work, specific laws are created for that industry. For example, the Fair Credit Reporting Act controls how consumer credit agencies use personal and financial information.

A notable data privacy case in the United States was *Riley v. California*, in which the court reached a unanimous decision that the examination of an individual's cell phone content during an arrest constituted a breach of their right to privacy. The court emphasized that a cell phone serves purposes beyond mere communication, as it contains personal private information, and the act of accessing this data infringes upon individual privacy rights.

Privacy involves the ability of individuals or groups to protect their information and to control their private sphere. It is recognized as a human right in Article 12 of the Universal Declaration of Human Rights (UDHR), which states that every individual has the right to privacy in regard to their private, family, and communications life, as well as the inviolability of their home and reputation. This right is also recognized in other international human rights instruments such as the ICCPR, ICPRAMW, and UNCRC. Data protection laws are therefore needed to protect this right. Privacy laws are made to prevent invasions of privacy such as the collection, storage, or sharing of personal data. Personal data includes any information that can identify an individual, which may be collected by a government or private entity.

The concept of privacy has long been acknowledged to be an integral part of the human rights package. It includes rights to privacy, rights to have secrets, the protection of one's physical self, rights to family, among others. It does not, however, include matters of private information related to public concern or is within the public record. Privacy is a very important requirement for leading a dignified life, but it is easier with new technologies and the widespread use of the internet to access and share someone's data, which might lead to its misuse. Phishing, viruses, and hacking are common cybercrimes that also pose threats to privacy. Therefore, good Data Protection Laws are required to deal with all these issues. In India, there are no comprehensive laws in place, but the Indian Constitution, IT Act 2000, Indian Contract Act, and Intellectual Property Laws offer protection. The original law was addressed by the introduction of the IT (Amendment) Act, 2008. Two important sections, Section 43A and Section 72A, were introduced to describe liabilities of companies and penalties for breaking contracts involving personal data. A number of initiatives are currently undergoing the process to strengthen data protection.

These include the proposed amendments in the Information Technology Act, the establishment of the Data Protection Commission of India, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules of 2011, and the Data (Privacy and Protection) Bill of 2019. Further legislative proposals over the years consist of the Prevention of Unsolicited Telephonic Calls and Protection of Privacy Bill presented by Baijayant Jay in the year 2009, besides other presented bills by Rajeev Chandrasekhar and Om Prakash Yadav. However, the Bill introduced in 2019 is still pending. Many issues arose after the judgment of the Supreme Court in the case of *K.S. Puttuswamy* on privacy, such as the Aadhaar Act and Section 377 of the Indian Penal Code, which was related to the consensual relationship between homosexuals. Currently, personal and sensitive data is often shared illegally with third parties, thus

making data a commodity. Another criticism against offshoring businesses is that they export personal data to other countries, which raises serious privacy concerns. This paper will examine whether the current legal framework in India is adequate to protect the privacy of its citizens or if new laws are required.

III. MAIN BODY

EVOLUTION OF THE RIGHT TO PRIVACY AS FUNDAMENTAL RIGHT IN INDIA

The Constitution does not specifically define what privacy is, but privacy can be said to be the right of an individual to live without interference and to not have his personal matters disturbed or left alone. Regrettably, most people are unaware of this right or cannot enjoy it to its fullest extent. Thus, to heighten awareness on the matter, several declarations and covenants were enacted regarding privacy as a human right. The Indian judiciary has also recognized privacy rights as a fundamental right under Article 21 of the Indian Constitution. Some of the landmark cases dealing with the right to privacy are as follows:

MP Sharma v. Satish Chandra

Here, the power of search and seizure was challenged as an invasion of the right to privacy. Yet, the court held that such search and seizure powers were not there to curtail the right of privacy. In addition, the court made it clear that such a case did not raise the question whether privacy was a constitutional right under Part III of the Constitution, and was not accorded the status of a fundamental right.

Kharak Singh v. State of UP

This case concerned whether the surveillance carried out by a state regulation violated the right of privacy. The Supreme Court declared that the regulation permitting night visits violated personal liberty. However, other provisions of the regulation were upheld because the right of privacy was not yet pronounced to be a fundamental right and Article 21 was not applicable. Judge SubhaRao did not agree to this argument that privacy must find a place under Article 21, though the right has yet to be fully recognized.

Govind v. State of Madhya Pradesh

In this case, the relevant statute allowing state surveillance at night was challenged and it was argued to be violative of privacy. The Supreme Court held that such kind of surveillance was not violative of any reasonable restrictions on the right of privacy and that such right could be suitably restricted based on public interest. For the first time, this decision had indicated the limitation to privacy rights.

Malak Singh v. State of Punjab & Haryana

Supreme Court stated that state surveillance, if not infringing the personal liberty but within the statutory limits, was permissible.

R. Rajagopalan v. State of Tamil Nadu

The court held that privacy is part and parcel of Article 21, which means every person has a right to protect private matters like education, family life, and reproductive choices. No one can publish information regarding these matters without the consent of the individual and would violate rights of privacy.

People's Union for Civil Liberty v Union of India

The court dealt with the question of whether telephone tapping was constitutional or a violation of privacy. It held that telephone conversations fall within personal life and that the tapping of such conversations without legal authority is a violation of privacy. However, telephone tapping is not unconstitutional if there is a law or regulation guiding the procedure, such as the Telegraph Act.

The Supreme Court recognized telephone and medical privacy but did not consider it a fundamental right at first. In 2012, K.S. Puttuswamy filed a petition challenging the constitutionality of the Aadhaar Act, which infringed on his privacy rights. The case led to the landmark judgments delivered by a nine-judge bench, which concluded that privacy is a part of Article 21 of the Constitution. The judgment overruled previous judgments in the cases of Kharak Singh and MP Sharma and stated factually that privacy is a legally recognized right under the Indian Constitution.

ISSUES UNDER THE HEAD OF PRIVACY

Several issues came to the fore, particularly after the landmark Aadhaar judgment relating to privacy: the constitutional validity of the Aadhaar Act, Section 377 of the IPC, and the legalities of live-in relationships without marriage. These issues would briefly be worthy of examination as thus:

Aadhaar Scheme

The Aadhaar scheme is a welfare initiative by the Government, which was introduced in 2009 to deliver direct benefits to Indian citizens. It works as a unique identifier that allows citizens to access various government welfare services, such as LPG distribution and the Jan Dhan Yojana. Under the scheme, the Unique Identification Authority of India (UIDAI) assigns a 12-digit number to each individual based on demographic and biometric data, including name, address, sex, iris scan, and fingerprints.

The scheme had the following problems:

1. It came into existence through an executive order rather than a statutory law passed in Parliament.
2. Data collection remained a private enterprise with no guarantees of data safety.
3. There was nothing in the law pertaining to prosecution under misuse of information collected.

Such concerns were addressed by passing the Aadhaar Bill as a money bill in 2016 and later forming it into an Act. After the enactment of the act, various notifications made essential linking of Aadhaar with PAN cards, phone numbers, bank accounts, and other services.

As for the question of constitutional validity, the Supreme Court entertained pleas on the matter of infringement of privacy and had a bench of five judges before it. In a verdict with a 4:1 majority, the Court upheld the constitutional validity of the Aadhaar Act but struck down a few provisions that included Section 57, Section 47, and Section 33(2). As a consequence, private parties can no longer demand Aadhaar numbers, and the right to complain against both private parties and the government for violating their privacy has been granted to the citizens. In his dissenting judgment, Justice D.Y. Chandrachud argued that the Act was unconstitutional since it was passed as a money bill, thereby undermining the power of the Rajya Sabha and violating the constitutional structure.

Section 377 of the Indian Penal Code (IPC)

Section 377 of the IPC criminalizes unnatural sex. The petition was filed initially in the Delhi High Court by Naz Foundation. Dismissed initially, this issue once again gained prominence in the year 2009 when Delhi High Court decriminalized homosexuality among consenting adults. However, the Supreme Court of India reversed that verdict in the year 2013, in *Suresh*

Kumar Koushal v. Naz Foundation.

The matter was again taken up by a five-judge bench headed by CJI Dipak Mishra after several PILs. In a landmark judgment, on September 6, 2018, the bench partly struck down colonial-era provisions of Section 377 with a decriminalization of homosexuality. The court held that sexual relations fall within the privacy rights of people, which comes under Article 21 (Right to Life and Personal Liberty) of the Constitution. However, the State may impose reasonable restrictions in the interest of public welfare.

INDIAN LEGAL FRAMEWORK ON RIGHT TO PRIVACY

India does not have specific laws which exclusively deal with privacy and data protection. Nonetheless, there is an indirect legal framework, which addresses privacy-related issues. Besides from statutory protection, privacy is also granted protection under the Constitution of India. In other words, privacy rights, as well as personal data, can be protected through two channels:

1. Constitutional Protection

2. Statutory Protection

Constitutional Protection

Indian Constitution does not mention privacy as a fundamental right. It was implied to come under the protection afforded by Article 21, particularly the Right to Life and Personal Liberty, along with all rights guaranteed in Part III of the Constitution. The Puttuswamy case with a nine-judge bench identified the right to privacy as an Article 21 fundamental right. Constitutionally recognized, but not absolute, the right could be reasonably restricted under Article 19(2) in interest of public welfare, national security, and the like. This view was supported by the judiciary, since early debates on privacy began, though the minority always dominated. Based on this concept, Article 21 is integral to the Constitution because it accommodates diverse rights within itself to fulfill changing needs in society.

Protection at the Level of Statutes

This includes various laws in India, such as IT Act 2000, the Indian Contract Act 1872, Intellectual Property Laws, and Credit Information Companies Regulation Act 2015. Below is a very brief outline of the above laws:

IT Act, 2000

The Information Technology Act, 2000, is India's first legislation aiming to cover e-commerce, e-governance, and cybercrimes. Data protection is offered against unauthorized access to computer systems and networks. The important provisions are:

- Section 43: The act penalizes unauthorised use of computer data, for which imprisonment can extend up to three years or fine can extend up to ₹5 lakhs, or both.
- Section 65: This section describes the alteration or destruction of computer source code.
- Section 66: Punishment for altering or destroying information in computer resource without authorisation. Punishment would be three years of imprisonment, or a fine of ₹2 lakhs, or both.

Directors and managers of a company are liable in case such a company violates any of the provisions of the IT Act.

Parts not originally incorporated into the Act were added in 2008 and the amendments introduced them. Section 69(A) empowered the government to snoop on internet sites and block those it wishes and the Supreme Court held that to be constitutionally valid in 2015, with proper safeguards.

Indian Penal Code, 1860

Although the IPC does not make any specific provision for data violation breaches, some forms of the crime, including dishonest misappropriation of property as contained in Section 408, could be extended to cover breaches of privacy.

Intellectual Property Laws

The Copyright Act, 1957 deals with the intellectual property issues. For instance, it prohibits the unauthorized use of computer programs. Section 65 of the Act states that whoever uses infringing copies of software shall be imprisoned for a term of three years or shall pay a fine. The Copyright Act also protects the work of authors who spend time and resources in developing original content.

Credit Information Companies Regulation Act (CICRA)

The CICRA governs the collection and dissemination of credit-related information. Institutions that collect and maintain such information are liable for any unauthorized disclosure or alteration. The RBI has imposed strict norms of information privacy under this regulation.

Indian Contract Act, 1872

The Indian Contract Act, 1872 governs agreements between parties, including confidentiality clauses related to the disclosure of personal information. If an individual discloses confidential information without authorization, it may lead to a breach of contract and potential damages. This is particularly relevant in insurance contracts, where the unauthorized disclosure of personal data can result in legal consequences.

RECENT EFFORTS IN INDIA TOWARDS DATA PROTECTION

As data thefts and data breaches continued, an immense burden was cast on the government and industries to ensure that data was protected. Though many a legal framework came into being, there was still a need for effort in the following areas, of which some are mentioned here:

Proposed Amendment of the IT Act

The Ministry of Communication and Information Technology recommended amending the IT Act 2000 to safeguard information. In turn, those suggestions led to the enactment of the IT Amendment Act 2008, bringing with it fundamental provisions in regard to data protection in the shape of Section 43A and Section 72A. Such provisions are strictly penal in character and contain elements of both criminal and civil law. Still, the said amendment is not so far incorporated in the form of a provision in itself but had led to creating new privacy rules.

Later, the Ministry issued a declaration on the rules and provisions under Section 87 (I) (06), read with Section 43A, which deems it relevant for a data handler to follow reasonable practices of security while processing sensitive personal information. A failure to observe the above rules would invite liabilities in the form of compensation, though the liability amount has not yet been defined. These apply to sensitive personal data, like credit/debit card information, passwords, biometric data, and health information. It defines that data available freely in the public domain or free to the public is not SPD.

The rules also require bodies corporate or their representatives to follow proper security procedures when handling sensitive personal data. If a violation occurs and harm is caused, the corporate body may be liable for compensation to the affected individual. In India, these rules represent a new approach to data protection laws, divided into three groups: the body corporate, the information provider, and the government.

Key features of the rules include:

- Rule 4: The body corporate shall host on its website a privacy policy, which describes what data the company collects and why it's being collected together with other details deemed essential.
- Rule 5: The body corporate cannot collect sensitive personal information without the provider's consent and must ensure that such data is collected for lawful purposes, used only for the specified reasons, and stored for no longer than necessary. The body corporate must also secure this information and set up a grievance redressal mechanism.
- Rule 6: Before disclosing sensitive information to third parties, the body corporate must obtain consent from the provider. However, data can be shared with government agencies without prior consent if mandated by law.
- Rule 8: The body corporate shall adopt reasonable security practices. This includes adopting ISO security standards, but the government may permit other practices in lieu of this. An independent auditor shall be authorized by the government to audit these practices every year.

Data Security Council of India

NASSCOM constituted the Data Security Council of India as a self-regulatory body that helps the industry to establish and enforce data security and privacy standards. It aims to create an awareness in the minds of all stakeholders about data privacy issues and provides a knowledge-sharing forum about data security. It is a not-for-profit organization where independent directors along with industry experts are on the board, and entities like IT-enabled services companies, academic institutions, and research bodies can be members.

National Do Not Call Services

With increased awareness of privacy, especially telephone numbers, the Telecom Regulatory Authority of India introduced the National Do Not Call registers. Subscribers can get themselves registered on the National Do Not Call registers so that they do not receive unsolicited calls from telemarketers.

PERSONAL DATA PROTECTION BILL, 2019

On 11 December 2019, the Personal Data Protection Bill was introduced by Minister of Electronics and Information Technology, Mr. Ravi Shankar, in Lok Sabha. The Bill focuses on establishing an overarching data protection regime, filling current gaps, and providing statutory protections. Prior to this, the Bill had been presented twice in Parliament in 2017 and 2018.

The Bill adds several salient features such as the obligation upon the data intermediaries to ensure protection of the collected data by security measures and to immediately inform about the breach of the data within a reasonable time, grievance redressal, and penal provisions for the Data Protection Officer and the DPPA to handle grievances against data collectors and processors. The Bill would allow citizens to file grievances against both private and governmental organizations for infringing privacy. They will be required to obtain explicit consent before handling sensitive or personal data. Even punitive measures like increased data breach fines are suggested by the Bill.

Although it is not enacted yet, it is considered as the first step toward comprehensive data protection, and if the Bill is enacted, it is going to create a highly effective legal framework in the future.

Specific Privacy Law

Despite the available legal framework and measures taken by the government, existing legislation does not provide proper protection to the personal privacy rights of individuals or their data. Besides, various gaps in the laws, for instance, IT Act and the 2011 Rules, emphasize the need for special laws. In this respect, the above points can be elaborated as follows:

GAPS IN THE EXISTING LEGAL FRAMEWORK

- Proposed Amendments in the IT Act:** The proposed amendments, including the insertion of Sections 48A and 72A, have not brought any significant changes to the original IT Act. The Standing Committee's comments on the amendments were only received by the Ministry of Parliamentary Affairs and have yet to be implemented.
- Does not Address the Root Concerns in Data Protection:** Proposed amendments fail to address fundamental concerns in data protection, including handling sensitive personal data, how data is treated, and the process involved in processing data.
- Narrow Scope of 2011 Rules:** The MCIT, through its rules of 2011, under Sections 87(2)(06) and 43A, essentially govern body corporates or other Indian entities. The rules are not applicable to state authorities. Liability and compensation would arise in case of violation under Section 43A, though the scope of this liability is yet undefined.
- Lack of Compliance from State-Owned Enterprises:** Rule 4 of the 2011 Rules states that private sector service providers such as Vodafone India and Bharti Airtel must make available their privacy policies on their individual websites. There has been a complete lack of action on part of the state-owned enterprises, leading

one to infer that there is very little concern towards data protection. Thus, these principles would remain ineffective.

- Little Regulatory Overhead in Respect of Non sensitive Information: Though the 2011 Rules pertain to sensitive personal information, such as passwords, medical data, and biometric information, the Indian rules do not govern much about non-sensitive information. Moreover, extraterritorial jurisdiction by Indian laws is not extensive; hence, there is a vagueness in the application of the IT Act or Privacy Rules on foreign firms, such as those operating from the US, gathering sensitive personal data from Indians.

- Other Legal Framework Limitations:

No All-inclusive Law on Private Rights: There is no overarching law that specifically deals with private rights pertaining to data protection.

No Clarity on Categorization: No categorization is provided to distinguish between private, public, and sensitive information.

Inadequate Procedures: No procedure definition of creation, processing, transmission, and storage.

Lack of Defined Norms on Quality of Data: There is no well-defined legal framework to refer to in regard to terms like data quality, proportionality, and data transparency.

Lack of Legal Framework on Data Flow across Border: The law does not contain adequate provisions with regard to management of data which flows across borders.

Against these lacunas found in the prevailing legal framework, it can easily be understood that there is a dire need of specific privacy and data protection legislations. In light of the fact that corporate bodies collect increasingly large volumes of customer information at a fast-growing rate, particularly in this rapidly globalized era of information technologies, internet services, and BPO operations, it is extremely important to have stringent data protection laws enacted. Such laws should encompass the international flow of data as well as safeguard rights to privacy and completely safeguard their data.

CONCLUSION AND SUGGESTIONS

Right to Privacy has been a Fundamental Right due to several rulings by the Judiciary. However, with the speed of technological growth, which is fuelled by globalization, comes a question: do we still have privacy in our lives? Privacy is an important right that enables us to lead a dignified life, make our own decisions, and grow as individuals. Thus, it is imperative to protect this right.

Technology has already become part and parcel of life today. Though it has ushered in enormous benefits, new threats to society include cybercrimes, data theft, and the subsequent misuse of data, which directly impacts our personal privacy. As we daily go about, we have to give information that borders on personal issues to both government agencies and private establishments as a precursor to getting the service. Doing so puts the information at the risk of theft or misuse-for example, in a country like India, which does not enforce proper Data Protection Laws. Of course, there are a few laws presently, like the IT Act, Criminal Law, and Intellectual Property Law, but they indirectly address the issue and are not very effective. If someone illegitimately uses

or leaks our data, then it can be called a "Breach of Privacy." Besides, loopholes exist in the existing laws. For example, no service provider or

data handler can be liable for any breach of data if they can prove that they didn't even know that the data was mishandled. To ensure that our data is not mishandled, we need a stronger Data Protection Law.

The Supreme Court has ruled that privacy under Article 21 of the Constitution is a Fundamental Right but declaring it does not solve the problem. People must know what their rights are and what to do in case of breach of privacy. If they do not know their rights, they may not be able to take steps to seek justice. Thus, people can only lead a dignified life if they know their rights. Where personal privacy was once the issue, today, data privacy also needs to be considered. The government should devise an efficient system that will quickly alert authorities when privacy is threatened. Legislators should pass laws and regulations to ensure that the data collected is protected. Such databases hold information that must be highly secured in a way that even experts cannot access such information without any authorization. Such data must be accessed only by authorized people only for the benefit of the people.

Additionally, the authorities responsible for collecting, processing, and storing data should be held accountable. There must also be penalties, including fines and imprisonment, to deter unauthorized individuals from mishandling personal data. Some experts have suggested replacing biometric data collection with smart cards, which would be optional. Smart cards require a PIN and would only work with the person's cooperation, ensuring that their identification is not misused. Once a smart card is discarded, it cannot be used again to identify any individual. The use of smart cards may reduce the chances of criminals, terrorists, or foreign governments using biometric data to trace Indian citizens.

REFERENCES

Justice K.S. Puttaswamy (Retd.) v. Union of India, Writ Petition (Civil) No. 494 of 2012, Supreme Court of India. (2017). Retrieved from https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_IndiaiPleaders+2DLA Piper Data Protection+2Wikipedia+2

Kumari, S. (2023). Different aspects of right to privacy under Article 21. iPleaders. Retrieved from <https://blog.ipleaders.in/different-aspects-of-right-to-privacy-under-article-21/>iPleaders

Carnegie Endowment for International Peace. (2023). Understanding India's new data protection law. Retrieved from <https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law>Carnegie Endowment

DLA Piper. (2025). Data protection laws in India. Retrieved from <https://www.dlapiperdataprotection.com/index.html?c=IN&t=law>DLA Piper Data Protection

Supreme Court Observer. (n.d.). Justice K.S. Puttaswamy (Retd.) v. Union of India – Background. Retrieved May 19, 2025, from <https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/> Supreme Court Observer

LawBhoomi. (2024, December 15). M.P. Sharma & Ors vs. Satish Chandra & Ors. Retrieved May 19, 2025, from <https://lawbhoomi.com/m-p-sharma-ors-vs-satish-chandra-ors/> LawBhoomi

Global Freedom of Expression. (n.d.). Kharak Singh v. State of Uttar Pradesh. Retrieved May 19, 2025, from <https://globalfreedomofexpression.columbia.edu/cases/singh-v-uttar-pradesh/> Global Freedom of Expression+1 Global Freedom of Expression+1

iPleaders. (n.d.). Govind vs. State of Madhya Pradesh. Retrieved May 19, 2025, from <https://blog.ipleaders.in/govind-versus-state-of-madhya-pradesh/> iPleaders

Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017). Supreme Court of India, (2017) 10 SCC 1. Retrieved from <https://indiankanoon.org/doc/127517806/>

M.P. Sharma v. Satish Chandra, District Magistrate, Delhi, (1954). Supreme Court of India, AIR 1954 SC 300. Retrieved from <https://indiankanoon.org/doc/1618254/>

Kharak Singh v. State of Uttar Pradesh, (1963). Supreme Court of India, AIR 1963 SC 1295. Retrieved from <https://indiankanoon.org/doc/619152/>

Gobind v. State of Madhya Pradesh, (1975). Supreme Court of India, AIR 1975 SC 1378. Retrieved from <https://indiankanoon.org/doc/1752241/>

R. Rajagopal v. State of Tamil Nadu, (1994). Supreme Court of India, AIR 1995 SC 264. Retrieved from <https://indiankanoon.org/doc/499918/>

People's Union for Civil Liberties (PUCL) v. Union of India, (1997). Supreme Court of India, AIR 1997 SC 568. Retrieved from <https://indiankanoon.org/doc/539407/>

A.K. Gopalan v. State of Madras, (1950). Supreme Court of India, AIR 1950 SC 27. Retrieved from <https://indiankanoon.org/doc/1294814/>

R.C. Cooper v. Union of India, (1970). Supreme Court of India, AIR 1970 SC 564. Retrieved from <https://indiankanoon.org/doc/1296073/>

Maneka Gandhi v. Union of India, (1978). Supreme Court of India, AIR 1978 SC 597. Retrieved from <https://indiankanoon.org/doc/1766147/>

Vishaka v. State of Rajasthan, (1997). Supreme Court of India, AIR 1997 SC 3011. <https://indiankanoon.org/doc/1031794/>

Universal Declaration of Human Rights. (1948). United Nations General Assembly, Article 12. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>

International Covenant on Civil and Political Rights. (1966). United Nations General Assembly, Article 17. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW). (1979). United Nations. <https://www.un.org/womenwatch/daw/cedaw/>

Privacy Act of 1974, 5 U.S.C. § 552a. (United States). <https://www.justice.gov/opcl/privacy-act-1974>

Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100–503, 102 Stat. 2507. (United States). <https://www.congress.gov/bill/100th-congress/house-bill/4938>

Fair Credit Reporting Act, 15 U.S.C. § 1681. (United States). <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>

Riley v. California, 573 U.S. 373 (2014). Supreme Court of the United States. <https://www.oyez.org/cases/2013/13-132>

Information Technology Act, 2000 (India). <https://www.indiacode.nic.in/handle/123456789/1999>

Information Technology (Amendment) Act, 2008 (India). https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (India). [https://www.meity.gov.in/writereaddata/files/GSR313E_10511\(1\).pdf](https://www.meity.gov.in/writereaddata/files/GSR313E_10511(1).pdf)

Data (Privacy and Protection) Bill, 2019 (India). Retrieved from PRS India. <https://prsindia.org/billtrack/data-privacy-and-protection-bill-2019>

Jay, B. P. (2009). The Prevention of Unsolicited Telephonic Calls and Protection of Privacy Bill, 2009. Retrieved from Lok Sabha Archives.

Chandrasekhar, R. (Proposed). Right to Privacy Bill (Unpassed). Retrieved from Rajya Sabha Records.

Indian Constitution. (1950). Article 21 & Article 51. <https://legislative.gov.in/constitution-of-india>

UIDAI (Unique Identification Authority of India). (n.d.). About Aadhaar. <https://uidai.gov.in/>

Supreme Court Observer. (n.d.). Suresh Kumar Koushal v. Naz Foundation – Section 377 & LGBT Rights Case. Retrieved May 19, 2025, from <https://www.scobserver.in/cases/suresh-kumar-koushal-v-naz-foundation-section-377-lgbt-rights-case/>

Naz Foundation v. Government of NCT of Delhi, (2009). Delhi High Court, WP(C) No.7455/2001. <https://indiankanoon.org/doc/1004723/>

Section 377 of the Indian Penal Code. (1860). Indian Penal Code. <https://indiankanoon.org/doc/1836974/>

The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. <https://indiankanoon.org/doc/96643240/>

Chandrachud, D.Y. (2018). Dissenting Opinion in K.S. Puttaswamy v. Union of India, Aadhaar Judgment. (As cited in SCC and SC Observer summaries). <https://www.scobserver.in/>