# A SURVEY OF THE PRIVACY RIGHTS GRANTED BY ARTICLE 21 OF THE INDIAN CONSTITUTION

**Nandini Sharma***

## ABSTRACT

*Around the world, the right to privacy has become widely recognised as a fundamental human right. In India, too, Article 21 of the Indian Constitution recognises privacy as a Fundamental Right. The security of data, which in today's modern and globalised society has become particularly challenging to achieve, is directly tied to the right to privacy. Further, the lack of legal protection for this Right has made it easy for the ruling majority to violate privacy rights through discriminatory legislation. This Right was not initially acknowledged in India as a Fundamental Right, and no special data protection law was passed to protect citizens' right to Privacy. At the same time, there have been several claims that the Indian government and private commercial entities occasionally violated citizens' right to privacy. Such claims were also brought before the courts of law, where the judges rendered important judgments that included rules and norms. To assess the level of security provided to Indian individuals regarding their right to privacy by the legal system, it is crucial to analyse all of these legislative changes relating to the right to privacy and data protection. However, it has been determined that the Indian Legal System has adequately recognised the Right to Privacy, and as a result, major steps have been made to prevent data theft despite the misuse of sensitive information. Significant advancements are still required to broaden the reach of data protection in the modern era and defend Indian residents' right to privacy.*

**Keywords:** Confidentiality, Sensitive Information, Personal Information, Data Protection, Public Interest.

*BA LLB (HONS.), FIFTH YEAR, IILM UNIVERSITY, GURUGRAM.

## INTRODUCTION

Privacy refers to a person's or a group's ability to keep information secret from others and to keep it to themselves. Additionally, it is a Human Right under Article 12 of the UDHR, which guarantees that no one has the right to have their privacy, correspondence, or family members invaded. Additionally, no one has the right to have their reputation or honour damaged. Every person has a right to protection from such interference. International human rights treaties specifically recognise the right to privacy as a human right. The identical phrase was adopted by the UNCRC, ICPRAMW, and ICCPR.[1] Data Protection Laws are necessary to protect this right to privacy. And these laws are referred to as "that collection of privacy laws, procedures, and policies" since their main goal is to lessen the invasion of one's privacy that may result from the preservation, gathering, and dissemination of personal information or data.[2] Additionally, "personal data" refers to any information that can be used to identify a person, whether it is gathered by a third party or the government. The idea of privacy has a long history and is a fundamental component of human rights, which are ingrained in every person from birth. They cannot be divided or treated as sacred. It covers things like the right to privacy, the right to privileged communication, the right to one's body being kept private, the right to one's sexual orientation, the right to have children, etc. The private right, information of public interest, or information in the form of a public record are not included in it. Privacy is crucial for living a respectable life. However, as new technologies develop and the internet becomes more widely used, it is now much simpler to access anyone's data and share it with a third party, potentially leading to data misuse. In addition, there are several cybercrime attacks in modern cultures, such as phishing, viruses, ransomware, hacking, spamming, etc. Therefore, we need stringent Data Protection Laws to prevent all such attacks. Although there aren't many comprehensive laws in India covering data protection, the Indian Constitution,[3] the IT Act of 2000,[4] the Indian Contract Act, and other laws of intellectual property, among others, enforce data protection. Additionally, the IT (Amendment) Act, 2008, was passed to address all the issues that the original Act did not. Additionally, it added two crucial clauses—Sections 43A and 72A—that discuss the responsibility of body corporations and the consequences of

[1] Gourab Roy Chowdhhury, 'Right to Privacy and Data Protection Issues in India' (2021) 8 *ISSN 2349-5162* 380

[2] Jayanta Boruah and Bandita Das, 'Right to Privacy and Data Protection under Indian Legal Regime' (2020) 1 *DME Journal of Law* https://dmejl.dme.ac.in/article/bandita-das/ accessed 16 March 2021; also available at SSRN https://ssrn.com/abstract=3827766

[3] Constitution of India, arts 19 and 21

[4] Information Technology Act 2000

violating a legal contract by discussing information. In addition, numerous steps are being taken to secure data, such as modifying the IT Act, creating the Data Protection Commission of India, passing the Data (Privacy and Protection) Bill in 2019 and the Information Technology (Reasonable Security Practises and Procedures and Sensitive Personal Data and Information).

Perhaps this is not the first time that a data protection bill has been presented to Parliament; in 2009, MP Baijayant Jay introduced a bill titled The Prevention of Unsolicited Telephonic Calls and Protection of Privacy to limit the number of calls that individuals or business promoters could make to people who had made it clear they did not want to receive them. Nevertheless, they made continuous calls. In addition to Baijayant Jay, numerous other people, including Rajeev Chandrasekhar (2010) and Om Prakash Yadav (2016), had previously introduced bills addressing citizen data privacy. The Bill of 2019 has not been put into effect yet, though. Again, numerous problems were taken into consideration following the Supreme Court's privacy ruling in the K.S. Puttuswamy case, including the legality of the Aadhaar Act and Section 377 of the IPC, which deals with consensual homosexuality. Currently, sharing data illegally with parties other than the intended recipient is becoming a means of generating cash. The material in question may be sensitive or personal. Additionally, it is claimed that a lot of offshoring business operations—where foreign corporations export a person's data—were carried out in India. These result in a serious privacy hazard. In order to determine if the Indian Legal Framework is adequate to protect the privacy of Indian Citizens or whether new rules need to be introduced, this article will analyse the Indian Legal Framework.

## RIGHT TO PRIVACY IDEAS

Privacy is defined as "An individual's Right to Control and Access His/her Personal Information" in Duhaime's Law Dictionary. This explanation explains privacy in a straightforward manner for laypeople. Simply put, it means that a person's right to privacy is complete control and uninterrupted access to his or her own personal information. His name, address, demographic information, personal matters, private space, etc., are all examples of personal information in this case. In his work, in his book, Gillian Black defines privacy as "the desire of an individual to be free from the intrusion of others." According to the definition, every person has the right to pursue his or her personal goals and conduct his or her private affairs without interference from others. Privacy is defined as "Every individual has the right to respect for his family and private life, his home and his correspondence" in Article 85 of the

European Convention on Human Rights. The Human Rights Convention is making a significant international effort to define the value of privacy in a person's life. According to the article, no government agency may intrude on a person's right to privacy unless doing so is permitted by law and is required for the security of the state, the welfare of the general public, or is vital to the nation's economic health. In a case, Justice Cory of the Canadian Supreme Court stated that privacy is "the situation of being alone, uninterrupted, and free from government scrutiny; safe from intervention or disturbance." A key component of privacy is the ability to bar visitors from the property. The right to privacy includes the freedom from interference or intrusion. Justice Dickson stated that a person's ability to choose when, how, and how much they will share their personal information might be characterised as privacy. A person must maintain the conviction that the State may only violate this right by secretly recording personal communications if it has established to the satisfaction of a judicial officer that an offence has been committed or is being committed and that communications monitoring provides evidence of the crime. In the case of J. K. S. Puttaswamy v. Union of India, the Hon'ble Supreme Court of India declared that "The privacy rights are guaranteed in accordance with Article 21 as an inherent component of the right to life and personal liberty and as a portion of the rights provided by Part III of the Constitution."

## SOCIAL IMPACTS OF DATA PROTECTION

"The only constant is change." According to this saying, evolution is the only thing that sustains humanity. The only thing on which people rely in the modern era is information. Through social internet platforms like Facebook, Skype, WhatsApp, and others, today's society is linked by a single informational thread. Nowadays, people rely so heavily on social media that they divulge every last detail of their lives to various users. People from all around the world may now share their data on these social media platforms, which have added a new dimension to the world. Therefore, it is crucial to safeguard data from misuse by people or the government by developing effective rules. Data protection is a top priority in the modern era because data is readily available everywhere and can be easily accessed without the owner's knowledge. Due to this, there is a great danger of crimes, including identity theft, hacking, and other online crimes. Information security is a part of data protection. People utilising computers have found ways to abuse or exploit information for a variety of reasons. A kind of communication reliant on the Internet is social media. There are numerous additional social media platforms, such as blogs, microblogs, wikis, webpages, widgets, and virtual worlds. However, social networking

services like Facebook, Twitter, WhatsApp, and others have grown significantly in popularity in recent years. Nevertheless, to use a social media platform and find other accounts, the person must first create a database. The main goal of this social media platform is to establish online connections. However, customers were unaware that such a privilege also leads to criminality.

## THE DEVELOPMENT OF THE PRIVACY RIGHT AS A FUNDAMENTAL RIGHT IN INDIA

The term "privacy" is not defined explicitly anywhere in the Constitution. However, what we know about privacy is that it refers to a person's freedom to live freely without interference, as well as their right to be left alone. The issue is that many individuals are exploited to exercise this freedom, and many of them are not even aware that it is a fundamental human right that cannot be curtailed. Therefore, several Declarations and Covenants have been implemented to educate individuals about their privacy rights, which are also Human Rights. Additionally, the Indian Judiciary considered privacy rights under Article 21 of Part III of the Constitution as a fundamental right. The following was a list of cases involving the right to privacy.

**M. P. Sharma v. Satish Chandra, (1954) SCR 1077:**[5] In this instance, the exercise of authority and seizure was contested due to a violation of the right to privacy. The higher judicial authority noted that the Constitution's framers did not intend to restrict the power of search and seizure as a breach of fundamental privacy rights, nonetheless. Additionally, the Supreme Court ruled that MP Sharma's case did not answer any queries about the Right to Privacy as a Fundamental Right under Part III of the Constitution. Therefore, under the Constitution, the right to privacy could not be recognised in this case.

**Kharak Singh v. State of U.P., (1964) SCR:**[6] In this instance, it was argued that the UP-regulation's surveillance violated Part III of the Constitution's Fundamental Rights. After hearing this, the Supreme Court invalidated Regulation 236(b) because it allowed for night-time surveillance by +visits, a blatant breach of ordered liberty and intrusion into a person's home. The other provisions of the rule were still valid, nevertheless, because Article 21 does not apply because diversity has not yet been acknowledged as a basic right under the provisions of the Constitution. In contrast, J. SubhaRao argued that although privacy was not recognised as a basic right, it was nevertheless a crucial component of Article 21.

[5] *MP Sharma v Satish Chandra* 1954 SCR 1077 (SC)
[6] *Kharak Singh v State of Uttar Pradesh* 1964 SCR 332 (SC)

**Gobind v. State of M.P., (1975) 2 SCC 148:**[7] Similar to the Kharak Singh case, the MP police's Regulations 855 and 856 were contested because the state's monitoring of habitual offenders' homes at night and their arrest of people they suspected of being criminals were violations of their right to privacy. A nighttime home visit would not necessarily be an unreasonable infringement on the right to privacy, the Supreme Court held in this case and declined to invalidate the regulations. It was the first instance in which it was determined that all privacy rights cannot be exercised. A just restriction based on a strong public interest might be possible.

**Malak Singh Etc v. State of Punjab & Haryana &ors (1981) AIR 760:**[8] In this case, the Supreme Court ruled that state monitoring conducted within legal bounds and without infringing on a citizen's right to personal liberty shall be valid and legal, provided there was no illegal interference.

**Rajagopal v. State of T.N., (1994) 6 SCC 632:**[9] In the case of R. Rajagopalan, the higher judiciary determined that every Indian citizen has the freedom to protect his or her privacy, regardless of whether it is connected to a child's education, the birth and upbringing of a child, reproduction, the decision to get married, starting a family, etc. No one may publish anything regarding the aforementioned subjects—whether it be truthful, complimentary, or critical—without first getting consent from the individual in question. And that would be a blatant invasion of privacy if someone did it.

**People's Union for Civil Liberties v. Union of India, (1996) 9 SCC 580:**[10] In this instance, it became apparent that phone tapping is unconstitutional because it violates the right to privacy. The Supreme Court ruled that phone conversations are protected by the right to privacy and can be made while seated anywhere, including at home or at work, because they are essential to a man's daily life. Thus, listening to phone conversations is against Article 21's right to privacy. The State may, however, record such talks if there is legislation defining the procedure to be followed for telephone tapping or if it complies with the Rules established under the Telegraph Act.

[7] *Gobind v State of Madhya Pradesh* (1975) 2 SCC 148 (SC)
[8] *Malak Singh v State of Punjab & Haryana* AIR 1981 SC 760
[9] *R Rajagopal v State of Tamil Nadu* (1994) 6 SCC 632 (SC)
[10] *People's Union for Civil Liberties v Union of India* (1996) 9 SCC 580 (SC)

**Justice K.S. Puttuswamy (Retd.) & Anr. v. Union of India & Ors. 494 of 2012, (2017) 10 SCC:**[11] The right to privacy was discussed along with the Unique Identity Scheme. Whether the Constitution guarantees such a right was the issue before the court. According to India's attorney general, privacy is not a fundamental right that Indian citizens are entitled to.

Different types of privacy, such as the privacy of phone conversations and medical information, emerged as a result of this legal interpretation. The majority of judges in the Kharak Singh and MP Sharma instances concluded that the right to privacy is not a basic right, hence it has not yet been recognised as such. But in 2012, K.S. Puttuswamy submitted a case to the Honourable Court challenging the constitutionality of the Aadhar Act on the grounds of privacy infringement. Since the Aadhar Act's legality was not an issue, the bench's nine members instead focused on the novel issue of whether the right to privacy is a fundamental right or not. A court of five judges later considered the case. In the Puttuswamy case, the Supreme Judicial

Authority, therefore, overturned the earlier rulings in the Kharak Singh and MP Sharma cases by ruling that the right to privacy is a fundamental right guaranteed by Part III of the Constitution, i.e., intrinsic in Article 21 itself. As a result of the discussion of all the cases above, it has been determined that the Right to Privacy has been designated a Fundamental Right of Persons under the Indian Constitution.

## PRIVACY-RELATED CONTROVERSIES

Following the Aadhaar privacy judgement, other concerns, including the constitutionality of the Aadhaar Act, Section 377 of the IPC, live-in relationships without marriage, etc., were taken into consideration. These issues are briefly analysed here.

**Aadhaar Scheme:** In order to directly benefit Indian citizens, the government introduced the Aadhaar welfare programme in 2009. It is a special identification number that must be presented as identification when applying for government assistance programmes like the Jan Dhan Yojana and the distribution of LPG. In accordance with the Supreme Court, the Unique Identification Authority of India (UIDAI) assigned 12-digit numbers to every person living in India after collecting demographic (name, address, sex, etc.) and biometric data about them. Several arguments were raised against this scheme:

[11] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1 (SC)

- First, an executive order rather than a law passed by parliament governed it;
- Second, there is no mechanism for data protection, and data collection is to be done by private organisations.
- Third, there is no mechanism for prosecution if somebody misuses the data or does not use it for the intended purpose.

As a result, in 2016, the Lok Sabha passed the Aadhaar Bill, which would later become an Act, to address all of these issues. The Aadhaar plan will receive legislative support as the Act's primary goal. Several notifications were published after it was passed, mandating the linkage of Aadhaar with PAN, phone, bank account, and other services. Many petitions contesting Aadhaar's constitutional legality due to privacy invasion were submitted in support of it before the Supreme Court, and it was considered by 5 judges on the bench, including CJI Dipak Mishra, Justice AK Sikri, A.M Khanwilkar, Ashok Bhushan, and Justice D.Y Chandrachud. And most recently, the Aadhaar Act was found to be constitutionally valid by a vote of 4:1. However, it repealed a few clauses, including Sections 57, 47, and 33(2), meaning that private companies can no longer request Aadhaar numbers and that people can now make complaints against businesses and the government for violating their rights. The Act is illegal because it violates section III of the Constitution, according to one of the five judges, J. Chandrachud. According to him, enacting Aadhaar as a financial bill that undermined the Rajya Sabha went against the constitutional design and was therefore a constitutional fraud.

**Indian Penal Code (IPC) Section 377:**[12] Section 377 of the IPC, which reflects unnatural sex, was originally brought up before the Delhi High Court by the Naz Foundation, but it was denied. But after 8 years, the Delhi High Court decriminalised homosexuality between consenting adults in 2009 in the Naz Foundation case. Yet again, the High Court of Delhi's ruling was overturned in the case of Suresh Kumar Koushal v. Naz Foundation in 2013. Following the filing of numerous petitions, a five-judge panel led by Chief Justice of India Dipak Mishra heard the issue once more in July. On September 6, 2018, the panel largely overturned the colonial-era restrictions of Section 377 of the IPC to decriminalise homosexuality. The argument put forth by the higher judicial authority is that sexual relations comprise an individual's right to privacy, which is guaranteed under Article 21 of the

[12] Indian Penal Code 1860, s 377

Constitution, or the right to life and personal liberty. The State may, however, impose reasonable limitations based on a compelling public interest.

## PRIVACY RIGHTS LEGAL FRAMEWORK IN INDIA

We are aware that there is currently no clear regulation in India that might deal with privacy and data protection. In the lack of such laws, there is nonetheless a legal structure that, although not directly addressing privacy and data protection, does so indirectly. In addition to statutory protection, the Indian Constitution also guarantees privacy protection. Therefore, two safeguards can be used to protect both personal data and privacy rights.

Privacy is not clearly or expressly recognised as a fundamental right in the Constitution. The Fundamental Right to Privacy is not expressly stated in the Indian Constitution generally, but it has been determined by judicial rulings that the right is protected by Part III of the Constitution. The following clauses are those that purport to have clauses relating to the right to privacy:

**Article 19:** Freedom of Speech and Expression – According to paragraph (a) of Article 19(1), "all citizens shall have the right to freedom of speech and expression." However, Article 19(2) justifies this by stating that it will not affect the application of any existing laws or prevent the State from enacting new laws, as long as those laws impose reasonable restrictions on the exercise of the right in the interests of India's sovereignty and integrity, state security, friendly relations with other nations, public order, decency, or morality.[13]

**Article 21:** Right to Life and Personal Liberty – Article 21 of the Indian Constitution[14] guarantees the right to privacy to both citizens and noncitizens. Although it does not expressly mention this, the Supreme Court stated that it does as a statutory justification. According to Article 21 of the Constitution, "No individual shall be denied his life or personal freedom except as provided by the procedure established by law." The foundation of the Indian people's freedom is Article 21. Since the Indian Constitution was adopted, there has been discussion over the phrase "procedure created by law" used in this article. The proper approach is to argue that the Fifth Amendment's due process clause and the significance of the operation generated by law are not all that dissimilar in the area of personal freedom.

[13] Constitution of India, art 19(1), art 19(2)
[14] Constitution of India, art 21

## PRIVACY RIGHTS UNDER DATA PROTECTION LAWS

The IT Act of 2000, the Indian Contract Act of 1872, the Intellectual Property Laws, the Credit Information Companies Regulation Act of 2015, and other pieces of law are those that deal with data protection in India at the present time. They are briefly addressed below: IT Act, 2000-

The IT Act of 2000 is India's pioneering IT law that aims to address cybercrimes, e-commerce, and e-governance. The legislation about data protection is another factor. The IT Act's main objective is to safeguard against data breaches brought on by computer data leaks. It has several restrictions, including those in Sections 65 and 66 that stop people from using computers, laptops, or other technology or information that belongs to them in an illegal way.

Any destruction of computer data is punishable under Section 43 of the aforementioned IT Act. According to this Section, anyone who utilises computer data improperly or illegally faces a punishment of three years in prison, a fine of five lakh rupees, or both.

Those who knowingly or willfully change, destroy, or conceal any computer source code are punishable under Section 65. Under Article 66, anyone who modifies or destroys data kept on a computer will be held accountable for their actions. The penalties outlined in these Sections are 3 years in prison, a fine of Rs. 2 lakhs, or both.

In addition, if a firm violates an IT Act provision, the company's management and directors are personally liable for the violation. The 2008 Act was subsequently passed to address the issues that the earlier Act did not address, as well as to aid in the further development of IT and related security issues. The new Amendment Act grants the Indian government authority under Section 69(A) to restrict electronic data stored in computer devices as well as to prohibit intercepting, monitoring, and decrypting computer systems and resources. However, there was a lot of discussion around this, and the Supreme Court later in 2015 ruled that Section 69(A), which allows the government to order the blocking of websites, is constitutionally lawful as long as proper procedural protections are in place.

**1860 Indian Penal Code:** The penal code does not explicitly address data privacy violations. Nevertheless, there are some offences from which it can be inferred that a penalty for privacy infringement exists, for instance, under Section 408 of the IPC, culpability arises from dishonest misappropriation of movable property.

**Law of Intellectual Property:** The Copyright Act of 1957[15] in India, the law addresses issues of copyright piracy (stealing) and imposes mandatory punishment that is proportionate to the gravity of the offence. According to Section 65 of the Act, anyone found using a computer or a copy of a computer programme that violates the law faces up to three years in prison or a fine. Additionally, when an author creates books, records, or broadcast programmes using data gathered from a different source while investing time, money, effort, and talent that constitutes work as defined by the Copyright Act, those works are protected as the author's copyright. As a result, any copyright violation may give rise to legal action from the outsourcing parent company under the Copyright Act.

**CICRA**

In India, any information about a person's credit must be gathered in accordance with the privacy standards outlined in the CICRA regulation.[16] In the event that the entities alter or disclose the data they have obtained, they shall be held accountable for it in accordance with this legislation. Any potential breach or manipulation of the data is the responsibility of the organisations that acquired and maintained the data. In India, CICRA has established a stringent system to protect the data about the credit and tenancy of businesses and individuals. Additionally, the RBI has informed of this Act's strict information privacy rules. Further, on the Supreme Court's directive in the Justice K.S. Puttaswamy case, the Indian government has formed a five-person committee under the leadership of Justice (Ret.) B.N. Srikrishna, a former justice of the Supreme Court, to develop a data protection bill. If the law is approved, it will be India's first comprehensive piece of legislation to protect online users' personal information against misuse by both state and non-state invaders. According to the official letter of the Srikrishna Committee, the government is cognizant of India's growing importance of data protection. It is crucial to ensure the growth of the digital economy while keeping people's private information safe and secure. The Personal Data Protection Bill, 2018, was the name of the committee's final report and draft data protection bill. A Data Protection Authority to oversee information processing operations is proposed by the Personal Data Protection Bill.

Additionally, it recognises the importance of protecting personal data in the context of the fundamental right to privacy as well as the need to create a shared culture that supports a secure

[15] Copyright Act 1957 (India)
[16] Credit Information Companies (Regulation) Act 2005 (India)

and honest digital economy, upholds the privacy of citizens' personal data, and promotes freedom, advancement, and creativity.

The Bill also states that it aims to safeguard people's right to be independent regarding their personal data, define appropriate areas for personal data flow and use, create a relationship of trust between people and institutions handling their private data, identify people's rights when their private information is processed, and create a framework for implementing organisational and technical measures.

**SUGGESTIONS**

The following recommendations have been made based on the aforementioned exchange:

The necessity for a constitutional amendment: a protected change is necessary so that specific guarantees of private rights can be made by introducing a new agreement. In order to provide side recognition for protection, such a shift is crucial. At precisely that point, the guarantee of individual freedom under the Article may become more and more important. Creating National Policy: India needs a comprehensive plan to guarantee that people have the freedom to manage their own information transmission and collection. This strategy's implementation of the key principles of practical information practises is essential.

In this way, the law would impose limitations on the gathering and utilisation of personal data by specific data users. Clients that collect personal information will be forced to clearly inform the public about why and how this information will be used. In order to implement, individual data clients would need to give users a way to stop their own data from spreading further. The online collection and production of personal data would be appropriately limited as needed. To guarantee the privacy of information and the trade of sensitive data on the Internet, whether categorised or personal, proper legal frameworks should protect educational privacy interests, self-governance interests, and information assurance interests.

Even while a complete confidentiality agreement is necessary to protect the individual's right to control the collection and transmission of personal information, this control must be used by the parties involved. Online users will, in any case, be held accountable for their electronic transactions. They should be aware of the content of these communications and take the necessary security precautions to protect their privacy, such as encryption. As people sign up for online services and participate in business transactions, they will also need to decide how

risky it is to have their personal information exposed. People will most likely take advantage of the numerous educational, social, and professional opportunities provided by the internet now and in the future by anticipating the risks of online use and using the recently illustrated reliable insurance schemes.

## CONCLUSION

As per my understanding, Article 21 of the Indian Constitution grants several privacy rights to individuals. These rights are essential for protecting the dignity, autonomy, and personal space of every citizen. The Supreme Court of India has consistently interpreted Article 21 expansively to safeguard various aspects of privacy through various judgments over the years.

The survey of privacy rights granted by Article 21 reveals that it encompasses a wide range of protections. These include the right to personal liberty, which guarantees freedom from arbitrary arrests an[17]d detentions. Additionally, Article 21 encompasses the right to privacy in one's own home, prohibiting unlawful intrusion by the state or any other entity.

Furthermore, the right to privacy under Article 21 extends to the ambit of informational privacy. This aspect protects individuals from unauthorised collection, use, or disclosure of their personal data. It ensures that individuals have control over the dissemination of their sensitive information. The right to privacy also encompasses bodily integrity and autonomy. It safeguards an individual's right to make decisions regarding their own body, including reproductive choices, medical treatment, and sexual orientation. Article 21 acknowledges and protects the individual's right to live a life of dignity, free from interference or coercion.

The Supreme Court of India has recognised that privacy is not an absolute right and may be subject to reasonable restrictions in certain circumstances. However, any such restrictions must be just, fair, and reasonable, and must serve a legitimate state interest. The survey of privacy rights granted by Article 21 emphasises the importance of privacy as a fundamental right for every individual in India. It acknowledges that privacy is crucial for the development of personal identity, autonomy, and the exercise of other fundamental rights.

It is important to note that the interpretation and scope of privacy rights under Article 21 may evolve, as new challenges and advancements in technology and society arise. The courts, legislative bodies, and society as a whole will continue to grapple with striking the right balance between individual privacy and the legitimate interests of the state.

Overall, the privacy rights granted by Article 21 of the Indian Constitution are vital for protecting individual freedoms and ensuring a democratic and inclusive society. These rights must be respected, upheld, and promoted by all stakeholders to safeguard the privacy and dignity of every citizen.