

## **RIGHT TO PRIVACY INHERENT IN LIFE AND LIBERTY ARTICLE 21 AND RELATED CONFLICTS**

*Written by Deepika Kulhari*

*NLU-J Alumni*

---

### **ABSTRACT**

There was a lot of discussion about privacy in the twenty-first century because there were so many things that needed to be done to protect people's data and civil rights, even if they were LGBT. They are both necessary and sufficient components of the Constitution's "fundamental rights." Everyone can do the same thing, whether they are wealthy or impoverished, and whether they have a large sum of money or a small sum of money. Finally, it is vital to develop one's individuality, integrity, and dignity. This is owing to the fact that one's actions determine these things. Although it is not a right that can be taken away, any incursion must be legal, necessary, and proportionate in order to protect this fundamental right. You won't be able to do it if you break the law. The Indian Constitution explicitly provides that privacy is protected under Article 21. This research looks at the history of privacy through a variety of judicial instances that show that privacy is a constitutionally protected right. Much of the paper is devoted to explaining how this right came to be recognised as a legal fundamental right. Because we have so much information at our fingertips, privacy is especially important in this day and age. Our information does not have to be shared in its entirety. To grasp this, you must first comprehend why privacy is so important in this situation. In the twenty-first century, there are numerous new technologies that make it vital to protect this type of informational privacy.

### **INTRODUCTION**

One of the most important rights that people have is the right to privacy, which is protected by various international human rights agreements.<sup>1</sup> Respect for people's rights is essential in a democratic society. Other rights, such as the ability to openly express oneself, access information, and engage with other people or organisations, are also aided and reinforced.

Surveillance and censorship are two examples of practises that infringe on people's privacy rights. You can only do these things if they are lawful, necessary for achieving a legitimate goal, and reasonable in proportion to your desired outcome. Because modern technologies have made it feasible to capture, retain, and share personal data in previously inconceivable ways, people have the right to privacy.<sup>ii</sup> As a result, the right to privacy has been enlarged to encompass the responsibility of the government to protect personal information.<sup>iii</sup> Many international treaties include measures for the protection of personal information. Those rules have been integrated into the laws of several countries.<sup>iv</sup>

### **JUDICIAL INTERPRETATION OF THE FUNDAMENTAL RIGHT TO PRIVACY**

There is nothing unusual in the judicial enumeration of one right on the basis of another under the Constitution. It isn't considered weird by most people. This practise makes sense if Salmond's description of liberty as "incipient rights" is correct. If this is the case, this practise is permissible under Article 21. The process by which constitutional courts name and characterise the core of constitutional rights that are still in operation is known as enumeration. Some Fundamental Rights, as the Supreme Court has recognised, are essential over time.

Because personal liberty is the broadest stepping stone to the right to an education, judges have concluded that several unnamed rights fall under Article 21, which deals with personal liberty. Food and water are basic necessities for people. They need their own space and the ability to be alone. The right to privacy, like the right to life, should be made a basic right by judges.

In *Unnikrishnan, J.P. vs. State of A. P.*; A Constitution Bench of this Court held that several unenumerated rights fall within Article 21 since personal liberty is of widest amplitude on the way to affirming of a right to Education.<sup>v</sup>

“Just like food and water, people need privacy”. In the verdict of Right to privacy to be declared as Fundamental Right; opinion by individual judges are:

People have a right to die, according to Justice J. Chelameswar, which is part of their right to privacy. People have the right to refuse life-saving medical treatment or, if they so choose, to end their own lives. He didn't stop there: he also suggested that snooping on people's phones and hacking into their personal information fit under the category of privacy. He also talked

about how much food people consume and whether a woman can choose to end her pregnancy. Privacy, according to Justice D Y Chandrachud, protects an individual's right to be free. He stated during his speech that privacy is important because it allows people to be free and recognises the importance of having control over important elements of their lives.

Privacy and freedom, according to Justice S A Bobde, go hand in hand. As you can see, the right to privacy and the right to liberty are "inextricably interwoven," and any "diminution" would diminish people's rights. In addition to ensuring that people's right to privacy is protected, it is necessary to set reasonable limits on that right so that it does not become excessive.

The Supreme Court declared in *Mr X v. Hospital Z*, that the right to privacy in a doctor-patient encounter is not always absolute.<sup>vi</sup> If someone was sick at the time, healthy people would think it was appropriate to breach their secrecy or private rights. People who did not break the law should be allowed to live their lives without being harassed, according to the *Directorate of Revenue v. Mohd Nisar Holla*.<sup>vii</sup> The right to be left alone was ruled to be a right under Article 21 in the case of *Gobind v. State of M.P. (1975)*.<sup>viii</sup> The Supreme Court of India stated that the fundamental rights guaranteed by the Indian Constitution, particularly the right to liberty under Article 21 of the Constitution, would be violated if the words in *M.P. Sharma and Ors. v. Satish Chandra and Ors.*<sup>ix</sup> and *Kharak Singh v. State of U.P. and Ors.* were read literally and putatively as law.<sup>x</sup> This Court's subordinate courts could not ignore higher-ranking judges unless they demonstrated a good reason for not following their decisions. It would be desirable if future decisions respecting privacy rights by this Court were examined to see if they were valid and decided by a strong enough bench. According to Lord Denning, you must have the right to be alone in order to be accepted. This means that people should be able to keep their personal lives private under English law. It must first be broken in order to claim damages or get an injunction if it is broken. It should also be able to maintain the confidentiality of all letters and messages sent to it. Some of these rights were more powerful than others. Each one has its own set of rules. As a result, it was designed to take place when the public's desire to be open triumphed over the public's desire to keep things private or secret. When it came time for the Courts to rule, they did so in every case. There would be a new case to deal with when each case was resolved. As a result, there would be a significant amount of case law to review. || "Personal liberty" was used as a blanket word to cover any rights that protect "personal

liberties" but aren't covered by Article 19. (1). It was said that while Article 19(1) dealt with some freedoms, Article 21 dealt with the rest. If you live in a country where you have the right to privacy, things aren't always the same. Surveillance required by law does not always constitute a violation of that right. In the Ramlila Maidan Incident, Re (2012) 5 SCC 1, this is valid.

## **TELEPHONE TAPPING**

Due to their right to privacy, there was some disagreement about whether a person's phone might be used to eavesdrop on them. When their phones were tapped, many people were irritated, and it was a terrible experience for them. Article 21 of the Constitution protects the right to "life and personal liberty," which includes the right to privacy. When the facts of a particular case proved that a person had a right to privacy, Article 21 went into effect. This privilege cannot be changed unless the law permits it. A man should be able to talk on the phone whenever he wants. Even if a person calls from the privacy of their own home or business, they should be able to do so.<sup>xi</sup> This made it clear that, unless the law clearly stated otherwise, phone tapping would be prohibited under Article 21. The procedure should be fair in general. Article 19 guarantees that when someone speaks on the phone, they are exercising their right to free speech and expression. This would be in violation of Article 19(1), which provides that everyone has the right to free expression. Taping someone's phone or cell phone would be illegal. This has been the case since 1885, when Section 5(2) of the Telegraph Act made it legal for anybody in India to listen in on telephone calls. The grounds and reasons why an instruction to tap a phone would be allowed were given out in the Section when it was written. Even if the husband listens in on his wife's phone call without her consent, it is still a violation of her right to privacy.<sup>xii</sup>

## **UNIQUE IDENTITY CARD AND PRIVACY**

Article 21 of the Indian constitution stipulates that everyone has a fundamental right to privacy. The right to privacy safeguarded not only our passwords but also our most sensitive information, and UIDAI's UID initiative violated this right. The Unique Identification

Authority of India (UIDAI) was a government agency that issued UIDs to all citizens. Therefore, the question was whether UIDAI violated the right to privacy. The government agency UIDAI issued a unique identity card (UID) to each individual after collecting their fingerprints, iris patterns, names, addresses, birth dates, and other information. It was believed to be the most confidential information a person could possess because it incorporated biometric data. In 2010, however, a measure was introduced that would permit the sharing of biometrics information for the benefit of national security.

UIDAI violated the Right to Privacy by allowing government and private entities to obtain biometrics information for unique identification. This puts an individual's private information at danger, as it could be exploited for any purpose. People were also concerned about the security of biometrics data held in big quantities because it was simple to hack and delete the information. It wasn't until 2011 that the Planning Commission of India assembled a panel of specialists to examine Indian privacy laws in depth and recommend revisions, despite the fact that biometric data security was seen as one of the government's most critical duties. The committee's chairman, Justice Ajit P. Shah, developed a list of nine principles: notification, informed consent, limited collection and use, access and rectification, non-disclosure, security, openness, and responsibility. In *M.P. Sharma v. Satish Chandra*, AIR (1954) SC 300, the Attorney General supported his arguments in the Supreme Court by citing precedents about the police's authority to seize and examine private property. The Supreme Court ruled that UID violates the right to privacy and that anyone might waive this right by voluntarily controlling their biometrics data. This argument was rejected because it would violate fundamental rights, which could not be waived under any circumstances. This was said by the Supreme Court in the case *Basheshar Nath v. Commissioner of Income Tax*.<sup>xiii</sup> As we studied more about the subject, we discovered that the government's UIDAI programme directly affects private rights, which is a crucial component of its ongoing drive to alter fundamental rights. Getting an Aadhar card was a requirement for many government programmes, including Aadhar-based Direct Transfer Subsidy, Jan Dhan Yojana, Passport in 10 days, Digital locker, Voter Card Linking, Monthly Pension Provident Fund, Opening a bank account, and Digital Life Certificate SEBI facilities, and now you can't even get one. The primary concern was whether or not it violates the Right to Privacy.



Justice P.S. Puttaswamy, a retired Karnataka High Court judge, stated that there are no safeguards, penalties, or prohibitions against obtaining personal information. He also stated that the proposed government law had been rejected by the Standing Committee on Finance of the Parliament. The top courts in the United Kingdom and France have ruled that laws permitting the collection and storage of biometric information are illegal. The only way for the government to remedy this issue is to discontinue UIDAI's biometrics information supplying mechanism. This would not lead to any further privacy issues in the future. But eliminating the UID entirely would cost the government a great deal of time and money, therefore the only solution to solve all the difficulties was to eliminate only the biometric data and keep the generic data intact.<sup>xiv</sup>

## **RIGHT TO INFORMATION ACT & RIGHT TO PRIVACY**

Both the Right to Digital and the Right to Privacy are crucial human rights in today's information age. Usually, these two rights work in tandem to hold the government accountable to the people. New technology and behaviours pose a growing danger to privacy. The technologies make it easy to get and distribute personal information. Sensitive personal information is now frequently collected and utilised. Internet is used to distribute public records. The Right to Access to Information Act states that requesting information from government agencies is a fundamental human right (RTI). It derives from the freedom of expression right to "seek and receive knowledge" and is a globally recognised human right.<sup>xv</sup> The meaning of Section 8(1)(g) of the Right to Information Act of 2005 were discussed in *Bihar Public Service Commission v. Saiyed Hussain Abd Rizwi*. According to the law, a person who claimed to care about the public requested information from the Bihar Public Service Commission regarding a variety of matters relating to the two-day interviews conducted by the commission.<sup>xvi</sup> The Commission disclosed all information with the exception of the names of the interview panel members. The High Court ruled that the information must be made available to the public. Information that could endanger someone's life or safety, or the identification of a person who provided confidential information or assistance for law enforcement or security purposes, is prohibited by section 8(1)(g). It was decided that certain matters, particularly those pertaining to appointments, must remain confidential. The authority may obtain the information from those who provide it in confidence and with complete faith,

honesty, and loyalty. This information must be kept confidential, which is consistent with the notion of fiduciary capacity.

## CONCLUSION

In a world in which information technology is rapidly evolving, privacy must be a fundamental right. Part III of the Indian Constitution recognises the right to privacy, hence the decision of the Honorable Supreme Court in this area is lawful. In addition, when the Data Protection Act goes into effect, which is anticipated to occur shortly, the fundamental right to privacy will play a significant role in preserving both online data and informational privacy. Bentham also provided a legal justification for his pain and pleasure theories. Consequently, the government must consider ways to make more people happy and less sad. The government should not have unrestricted access to the personal information of its citizens. In addition, when deciding between invasion of privacy and public interest, attention should be made to determine which is more crucial. Individual demands cannot take precedence over public needs. The maxim "public welfare is the highest law" (*salus populi est suprema lex*) must be upheld in a democracy.

## REFERENCES

---

<sup>i</sup> Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

<sup>ii</sup> Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil and Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; See also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

<sup>iii</sup> Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17) See: A/HRC/WG.6/13/MAR/3, para. 37

<sup>iv</sup> As of December 2013, 101 countries had enacted data protection legislation. See: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map. Available at SSRN:<http://ssrn.com/abstract=1951416> or <http://dx.doi.org/10.2139/ssrn.1951416>

- 
- <sup>v</sup> Unnikrishnan, J.P. vs. State of A. P; 1993 AIR 217,1993 SCR (1) 594,1993 SCC (1) 645, JT 1993(1) 474,1993 SCALE (1) 290
- <sup>vi</sup> Mr X v. Hospital Z, (1998)8 SCC 296
- <sup>vii</sup> Directorate of Revenue v. Mohd Nisar Holla, (2008) 2 SCC 370.
- <sup>viii</sup> Gobind v. State of M.P. [(1975) 2 SCC 148].
- <sup>ix</sup> M.P. Sharma and Ors. v. Satish Chandra and Ors. 1954 AIR 300
- <sup>x</sup> Kharak Singh v. State of U.P. and Ors. 1963 SC 129
- <sup>xi</sup> S. N. Parikh, "Telephone-Tapping and Right to Privacy," Gujarat Law Herald, 1998, Vol. 8, pp. 12-24.
- <sup>xii</sup> Anila George, "Tapping Privacy: The Telephone Tapping Case," Lawyers Collective, June 1997, Vol. 12, pp. 28-29
- <sup>xiii</sup> Basheshar Nath v. Commissioner of Income Tax, AIR 1959 SC 149.
- <sup>xiv</sup> K.S. Puttaswamy (Retd.)and Ors. v. Union of India (UOI) and Ors,3
- <sup>xv</sup> Universal Declaration of Human Rights(UDHR), art.19
- <sup>xvi</sup> Bihar Public Service Commission v. Saiyed Hussain Abd Rizwi, Civil Appeal No. 9052 of 2012 arising out of SLP (C) No. 20217 of 2011