The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

RIGHT TO PRIVACY: WITH SPECIAL REFERENCE TO TELEPHONIC COMMUNICATION

~Babul Ashraf & Shishank Sharma

ABSTRACT:

The right to privacy has evolved in the digital era from a narrow protection against physical intrusion to a broader right covering informational autonomy and data protection. The growth of telecommunication technologies has intensified concerns such as surveillance, data misuse, and interception of communications. These challenges have necessitated stronger legal recognition and safeguards. Judicial interpretation has played a vital role in establishing privacy as a fundamental right and in developing principles to balance individual liberty with state interests. Thus, the modern concept of privacy reflects an ongoing effort to protect personal freedom in an increasingly digital and interconnected world.

Keywords: Right to Privacy, Data Protection, Telecommunication Technologies, Fundamental Rights

EVOLUTION OF THE RIGHT TO PRIVACY IN THE DIGITAL ERA:

The emergence of the right to privacy in the digital age can be considered revolutionary for legal theory and reflects the shift from a limited definition associated with physical invasions to a more intricate approach which embraces informational self-determination, data security and protection against ubiquitous digital surveillance. Traditionally, privacy was conceived as the individual's right to be protected from unauthorized physical invasion of one's private life. It was precisely defined in Samuel D. Warren's and Louis D. Brandeis' famous essay published in Harvard Law Review in 1890, which referred to privacy as "the right to be let alone." [1] At the moment, the dangers to one's privacy came mostly from invasive journalism and developments of photography and printing. Today, however, the advent of novel

communication technologies has greatly impacted the understanding of privacy, making it more vulnerable and requiring protection.

In the past, the constitutions did not have any specific mention about privacy in their constitution but made use of interpretation of other rights to imply this right. For example, in the constitution of the United States, rights related to privacy were implied through the Fourth Amendment that prohibits illegal search and seizure. By virtue of judicial interpretation, the Fourth Amendment covered some elements of privacy when there was any sort of surveillance and electronic communication involved. Additionally, in India, although there is no provision about privacy in the Indian constitution, it was implied by Article 21 that confers the right to life and personal liberty.[2]

[1] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" 4 Harvard Law Review 193 (1890).

[2] The Constitution of India, art. 21.

The emergence of digital communication technologies like the Internet, smartphone technologies, social media sites, cloud computing, and big data analysis has greatly changed the privacy landscape. While previously something that could be restricted to geographic location and limited scope in other times, the world of privacy has now been changed by digital communication technologies. One of the most important aspects of achieving this shift is communication technologies. Instant messaging programs, email programs, video conferencing applications, and social media sites produce huge amounts of data daily, including metadata regarding individuals' actions and social relationships.

The judiciary has had a significant impact on developing a right to privacy, such as the U.S. Supreme Court ruling in Carpenter v. United States.[3] The court decided that the government's collection of historic cell service towers to determine a person's location qualifies as a search under 4th Amendment rights. The Supreme Court determined that advances in technology have increased government's potential for accessing private information.

An important landmark in the history of privacy law in India came when the judgment in the case of Justice K.S. Puttaswamy (Retired) v. Union of India was delivered in 2017.[4] The case was decided by a nine-judge bench, and it was determined that privacy is a fundamental right that exists under Article 21 of the Indian Constitution, along with other provisions of the constitution. According to the ruling, it was found that the right to privacy is an important element of human dignity and freedom.

These developments in the courts have been supplemented by the implementation of data protection statutes that seek to control data processing in the digital age. This is illustrated by the enactment of the General Data Protection Regulation (GDPR) in the European Union in 2018, which has some of the most robust data protection laws in the world.[5] This legislation helps establish the basic tenets of data protection, such as legality, fairness, transparency, purpose specification, data minimization, and accountability. Furthermore, GDPR places a premium on informed consent.

The introduction of the Digital Personal Data Protection Act, 2023 in India represents a significant milestone that shows the country's commitment to setting up a comprehensive legal regime in respect of data protection.[6] Essentially, this statute is grounded in the basic principles enshrined in the Puttaswamy case and aims at achieving a proper equilibrium between individual interests, those of the State, and the digital economy as well. First of all, it sets forth a consent-based framework of data processing where the person becomes a "data principal" and acquires some rights, including receiving information about one's data, rectifying mistakes, and resolving issues. Secondly, it assigns the "data fiduciary" with some obligations to process and protect the data.

[3] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2018.

[6] Digital Personal Data Protection Act, 2023 (India).

In spite of all the above advances, however, there are still many challenges that need to be addressed in order to effectively safeguard privacy in today's world. First of all, the increasing use of artificial intelligence, machine learning, and algorithms raises the issue of their accountability and discrimination. Secondly, the international character of the Internet in the contemporary world means that any regulations applicable only on a national level will cause jurisdiction issues.

Lastly, the clash between national security and privacy concerns is also highly topical. In essence, the evolution of privacy law in today's digital age can be said to be the quest for a balance between advancements in technology and human rights. Originally, the law only provided a form of protection from physical invasion, but today it has developed into a multi-faceted concept, which includes data privacy and personal autonomy. The decision in Carpenter v. United States and the case of Justice K.S. Puttaswamy v. Union of India, along with statutes like the GDPR and Digital Personal Data Protection Act, 2023, show how privacy law has continued to evolve. In any case, the purpose of privacy law is to make sure that developments in technology do not undermine fundamental human rights.

DIGITAL COMMUNICATION TECHNOLOGIES AND CHALLENGES TO TRADITIONAL PRIVACY NOTIONS:

The the arrival of new technologies of communications in the era of digitization implies thatconcepts of privacy, which were centered on spatial distance, territoriality, and famously "the right to be left alone," have been fundamentally reconceptualized. Technologies of digital communication entail internet, technologies for smartphones, social networking sites, cloud computing technologies, IoT technologies, big data analytics, and AI-enabled surveillance systems, and allow an enormous amount of personal data to be collected, processed, stored, and distributed in real time, without having prior knowledge on the part of the person involved. While previous notions of privacy were founded on interaction and invasion of territory, modern technologies enable persistent and concealed surveillance that is not bound by either space or jurisdictional boundaries. The reasonable expectation of privacy, which underpinned numerous constitutional protections against governmental encroachment upon individuals' private spheres, was defined in the landmark case of Katz v. United States, 1967.[7]

The breakdown of the public/private split is an equally compelling challenge. While in the past privacy relied upon physical walls and invisibility, contemporary citizens generate

considerable digital footprints simply by using various devices, such as GPS information collected via smartphones, behavioral data stored on social networking websites, biometric information collected using wearables, and metadata recorded by messaging services. Contemporary technology allows for not only government but also private businesses to perform continuous monitoring. Such phenomena are well captured by the concept introduced by Shoshana Zuboff of "surveillance capitalism," when digital firms utilize human experiences for the benefit of creating predictive commodities, thus often violating personal freedom and dignity. Due to this, "the chilling effect" occurs, when individuals refrain from expressing themselves, making connections, or exploring new things online due to fear of profiling and manipulation.

Such a trend exposes several flaws in contemporary definitions of privacy. Contemporary approaches to privacy were not able to confront large-scale use of metadata, location data, and biometric data for predictive, profiling, and intervening activities conducted by governments and corporations. As Daniel J. Solove describes in his innovative work titled “Understanding Privacy,” privacy should not be regarded as an idea defined by just one principle, but rather a collection of problems associated with gathering, processing, distributing, and intrusion into information. In the context of the contemporary Internet era, all these issues pose challenges of unprecedented levels.[8] Transfer of data across national borders adds complications because information collected in one nation may be processed in another state. Furthermore, cybersecurity poses another challenge to privacy.

[7] Katz v. United States, 389 U.S. 347 (1967).

[8] Daniel J. Solove, *Understanding Privacy* (Harvard University Press 2008).

In its landmark ruling in the case of Justice K.S. Puttaswamy (Retd.) vs. Union of India (2017), the Supreme Court of India addressed the above issues head on. Privacy is a fundamental right, which flows out of the Right to Life and Personal Liberty under Article 21 of the Indian Constitution according to a verdict by a nine-judge bench. This case underscored the problems that arise due to the technological revolution with regard to data collection and surveillance activities. In other words, privacy includes the right to informational privacy, which involves exercising control over one’s data. It held that even though the right to privacy could not be absolute in nature, any government intervention had to satisfy the three-pronged test of legality, legitimacy, and proportionality.[9]

However, there is general academic agreement that approaching privacy as a private law right

alone would not suffice in today's world. According to academics, privacy is socially significant in safeguarding democracy from state abuse and corporatization. Taking into account the contemporary situation where algorithms can influence individuals' views and impact elections or conduct surveillance on a mass scale, new ways of privacy protection have to be developed, especially in respect of power dynamics. This issue is further complicated by the global nature of online platforms.

To conclude, the formulation of the idea of privacy in the digitalized world consists of more than technological and legal aspects. It is about re-positioning of human freedom and human dignity within the current communication system. Although some legal precedents have been created by important court rulings like Katz and Puttaswamy, new laws have been adopted to create an effective way for the security of people's data. Nonetheless, more research and study must be done in order to preserve the core of privacy.

Supra note 4.

DATA PROTECTION LAWS AND JUDICIAL SAFEGUARDS IN DIGITAL COMMUNICATIONS:

Because of the rapid development in the area of digital communication, the processes of generating, transferring, and storing personal data have been radically transformed; thus, severe risks emerge with regards to the privacy right protection. The modern digital environment involves constant transferring of personal data through various types of digital media such as instant messaging, social networking, cloud computing, telecommunications, and many more. Apart from creating a huge volume of metadata associated with the generation and transfer of data which may result in the violation of the privacy of personal data, digital media also collect behavioral data about the user. Consequently, the privacy concept has become that of controlling personal data rather than protecting it from invasion.

One such legislation passed in India to tackle the above-mentioned concerns is the Digital Personal Data Protection Act, 2023 (DPDP Act).[10] This act stresses the need for informed consent and accountability on the side of data fiduciaries and has a comprehensive structure regarding the processing of personal data. Furthermore, it ensures that personal data is only used for lawful purposes for which consent has been received. Hence, the DPDP Act makes sure that the principle of purpose limitation is being followed. Additionally, this legislation

has made provisions for the principle of data minimization by stressing the fact that only the minimum amount of data required for the particular purpose must be collected and processed. Data fiduciaries are required to take necessary steps in order to avoid any sort of data breach and inform the respective person in time about it.

Apart from the above-stated obligations, the DPDP Act provides a number of enforceable rights to the individuals. These rights have been referred to as rights of data principals. These rights include the right of access to data about the individual held by data fiduciaries, the right of rectification of any erroneous data, the right of erasure of any data that is not necessary, and the right to access an effective grievance redressal system. The legislature, through this enactment, also aims to empower the citizens and provide them a rights-based regime concerning their data. Furthermore, the ambit of this Act is not limited only within territorial boundaries as the Act applies to personal data processed outside India if it relates to the provision of goods or services within India.

The basis of this Act stems from several constitutional provisions particularly regarding the recognition of right to privacy as a fundamental right by the Supreme Court of India. In Justice K.S. Puttaswamy (Retd.) vs. Union of India,[11] a nine-judge bench concluded that the right to privacy was an essential aspect of Article 21 of the Constitution.[12] Privacy was characterized as having informational privacy, allowing an individual to control the dissemination and utilization of their personal data. Additionally, in cases where the state's actions that interfere with an individual's right to privacy can be justified, a tripartite analysis

[10] *Supra* note 6.

[11] *Supra* note 4.

[12] *Supra* note 2.

was used, requiring that these actions meet the following requirements: legality, legitimacy of state purposes, and proportionality towards achieving the objective.

Judicial decisions in other courts have also played an important role in the history of the privacy law in the digital communications sector. Such a judicial decision can be seen in the judgment delivered by the US Supreme Court in the case of Carpenter v. United States.[13] This decision states that obtaining the historic cell-site location information (CSLI) of the law enforcement agencies constitutes a search under the Fourth Amendment. Its significance lies in the fact that the US Supreme Court has stated that CSLI provides "an intimate window into a person's life" through the disclosure of the movements of a person during a particular period.[14] The

significance of this judgment is further strengthened due to the fact that it marks the first instance where the third-party doctrine has been abandoned in the field of digital information.

Worldwide, the General Data Protection Regulation (GDPR) in the European Union, which was implemented in 2018, serves as a good example of a law that can serve as a benchmark in comparing other data privacy regulations in various countries. The GDPR provides an extensive legal framework regarding issues such as legality, fairness, transparency, purpose limitation, and accountability.[15] In addition, it ensures that individuals are given certain rights such as access to, rectification of, erasure of, and restriction of data processing and the importance of giving informed consent to process personal information. Other duties include carrying out data protection impact assessment, appointing a data protection officer, and notification of data breach. Moreover, the GDPR applies outside territorial jurisdiction since it not only applies to organizations within the European Union but also those operating outside the region and dealing with the processing of data on people residing in the European Union.

In this case, there can be no doubt that the role of the State is critical in ensuring that development and innovation are accompanied by a strong protection of fundamental human rights. Indeed, it would be essential that the framework created by the DPDP Act be enforced and updated continuously. Additionally, judicial scrutiny must be sought so as to guarantee that the infringement on privacy is indeed proportionate.

In conclusion, developments within digital communication technology have necessitated the re-evaluation of the idea of privacy and have thus led to the establishment of extensive legal frameworks and constitutions that protect individual freedoms. The DPDP Act, Puttaswamy decision, Carpenter v United States, and GDPR all suggest that the world is moving towards recognizing privacy as a fundamental legal right. It can be observed that there must be a balance between progress and humanity in this modern world.

[13] *Supra* note 3.

[14] ibid

[15] *Supra* note 5.

BALANCING PRIVACY RIGHTS AND STATE INTERESTS IN THE DIGITAL AGE:

With the advent of the digital era, whereby information is continually being produced from sources such as smartphones, instant messaging, social networking sites, and

telecommunications, involving information on matters such as location, metadata, behavioral patterns, and personal interactions, the question of ensuring that the fundamental human right of privacy is not violated by the government's interest in maintaining the security of its citizens emerges as one of the most important constitutional questions of our day. It appears that technology has turned all of our activities into data that the State can easily access, leading to the potential development of the surveillance state despite the necessity of the State's role in keeping its citizens safe.[16]

In the historic decision of Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 by a nine-judge bench of the Supreme Court of India, legal guidelines have been established for what can be a very complicated issue. The Supreme Court held that the Right to Privacy forms an essential and integral part of the Right to Life & Personal Liberty, as stipulated in Article 21 of the Constitution of India. Additionally, they recognised that `Information Privacy` comprises an inherent part of such rights; and as such included an element of control over how will information is processed and dispersed between people outside the home. A key element of this decision was that the Right to Privacy is not an absolute right. Violation of the Right to Privacy (an infringement) by the Government must meet the following criteria: there must be a legitimate law in existence, there must be an urgency of state necessity, and finally, the violation must be proportionate to the infringement.

The principle of proportionality, derived from global constitutional jurisprudence yet modified according to the Indian context, has assumed an importance of its own in the area of digital communications. Technological advancements, such as the interception of telecommunications under Section 5(2) of the Indian Telegraph Act, 1885, and interception and decoding of electronic information under Section 69 of the Information Technology Act, 2000,[17] provide the state with access to extremely private information with very little resistance. The Information Technology Act in particular has reduced the bar in comparison to the Telegraph Act by doing away with the requirement of a 'public emergency' or 'public safety', as the act becomes 'necessary or expedient' only on the basis of certain grounds, such as investigating crimes. Such powers, without any checks, might create a situation where the exercise of the right to speech and dissent, freedom of journalism, and personal autonomy might become impossible.[18]

[16] Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018).

[17] Information Technology Act, 2000 (Act 21 of 2000), s. 69.

[18] The Indian Telegraph Act, 1885 (Act 13 of 1885), s. 5(2)

The DPDP Act, 2023 attempts to give effect to the principles enshrined in Puttaswamy in India's digital domain. According to the DPDP Act, the processing of personal data must be carried out in accordance with the principles of informed consent and imposes the duties of purpose limitation, data minimization, and appropriate security safeguards on data fiduciaries. Furthermore, the DPDP Act enables individuals to exercise the rights of access, correction, erasure, and grievance redressal. Nevertheless, the DPDP Act attempts to reconcile these rights with the interests of the state through the exclusion of certain state instrumentalities from such clauses in accordance with Section 17. Under Section 17, the provisions of the DPDP Act will not apply in respect of the processing of personal data by the notified state instrumentalities for matters relating to the sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order, or the prevention of incitement to offenses relating to any such matter. The Central Government may also use the data provided by such instrumentalities.[19]

Despite the recognition of state compulsions in this day and age of cyber-attacks, terrorism, and criminal syndicates in granting exemptions to the State, one cannot ignore the fact that the wide and loose nature of the exemptions along with the lack of mandatory judicial review for many surveillance measures grants a clear upper hand to the State. As opposed to the strict conditions imposed by the Supreme Court of India under People's Union for Civil Liberties vs Union of India, 1997 on telephone intercepts,[20] which required authorization by a high authority, review committees, and destruction of any unnecessary information, the present system of digital surveillance under the Information Technology Act is largely driven by executive discretion without any transparency or accountability. In addition to the absence of legislation or oversight on surveillance, the lack of a Privacy Commissioner with judicial powers leaves a lot to be desired when one considers the possibility of misusing the information collected through surveillance.

Comparative jurisprudence may provide some guidance regarding the potential avenues for improvement. The US Supreme Court in the case of Carpenter v. United States (2018) grappled with similar problems stemming from innovations in digital communication technology. The Court ruled that the gathering of historic cell site location information (CSLI) through which an enormous volume of information about one's whereabouts can be gathered over extended periods amounts to a search protected under the Fourth Amendment.

Chief Justice Roberts in his majority opinion highlighted how CSLI yields "encyclopedic" and "near-perfect surveillance" of one's life, disclosing private information that is much more intrusive than any traditional physical search. The Court refused to blindly apply the third-party doctrine derived from previous cases such as Smith v. Maryland[21] and United States v. Miller[22] to the current situation. It refused to accept that the use of a phone implies the voluntary assumption of risks regarding sharing private location data.

[19] *Supra* note 3, s. 17.

[20] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.

[21] *Smith v. Maryland*, 442 U.S. 735 (1979).

[22] *United States v. Miller*, 425 U.S. 435 (1976).

It is important to note the lessons learned from Carpenter case, which show that even information collected incidentally while participating in the digital communications network should enjoy a reasonable expectation of privacy upon aggregation and analysis. It is essential to have a warrant or similar legal procedure in place and not just an administrative order in cases where collection will take place over a long period of time or in large quantities, to the extent where all of the individual's life activities could be pieced together.

In India, the lack of such stringent procedural guarantees has been a source of criticism. The Central Monitoring System (CMS), Network Traffic Analysis (NETRA), and NATGRID allow centralized interception and monitoring of all communication through telecom and Internet service providers.[23] Although such measures help fight terrorism, cyber crime, and national security threats, there are concerns about their misuse, lack of transparency about the number of interceptions and their justification, and the lack of any mechanism for public disclosure. The exceptions allowed by the DPDP Act are legally justifiable, provided they are narrowly interpreted, following the Puttaswamy judgment. However, if not notified properly, they could easily serve as a cover for any activity without accountability, thus posing a threat to privacy and data protection. Judicial review is the last resort, yet it is very difficult to prevent abuse of power before the fact or remedy a breach after the fact.

In sum, the growing body of jurisprudence regarding the right to privacy in the context of digitization can be seen as a part of the development of the constitutional ethos in which there is enough room for the state to ensure the collective security of society by defending against increasingly advanced digital threats; however, any kind of unrestricted surveillance would

endanger the very ideals of human dignity, autonomy, and informational self-determination that underpin the notion of privacy. As technology becomes ever more advanced, with threats of artificial intelligence being utilized for predictive policing, biometric surveillance such as facial recognition software, and even quantum computing becoming a reality, the need to strike an appropriate balance in constitutional terms will be increasingly difficult.

[23] Ministry of Home Affairs, Government of India (CMS, NETRA, NATGRID Frameworks)