INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

EVOLVING JURISPRUDENCE ON DATA PROTECTION: A JUDICIAL PERSPECTIVE

AUTHOR - TAVISHEE DUBEY* & DR ARVIND P. BHANU**

* STUDENT OF LAW, AMITY LAW SCHOOL, NOIDA, UTTAR PRADESH

**FACULTY OF LAW, AMITY LAW SCHOOL, NOIDA, UTTAR PRADESH

BEST CITATION - TAVISHEE DUBEY & DR ARVIND P. BHANU, EVOLVING JURISPRUDENCE ON DATA PROTECTION: A JUDICIAL PERSPECTIVE *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (5) OF 2025, PG. 524-537, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

In the wake of increasing digitization and the proliferation of personal data collection by both state and private actors, the legal discourse surrounding data protection in India has witnessed significant evolution. This paper examines the judicial approach to data protection, with a particular focus on the role of the Indian judiciary in interpreting the right to privacy under Article 21 of the Constitution and shaping the trajectory of data protection laws, culminating in the enactment of the Digital Personal Data Protection (DPDP) Act, 2023. It critically analyzes landmark judgments, including *Justice K.S. Puttaswamy v. Union of India*, which recognized privacy as a fundamental right, and how this recognition laid the groundwork for legislative and regulatory frameworks for personal data protection.

The study explores the historical development of privacy jurisprudence in India, the inadequacies of the Information Technology Act, 2000, and the transition toward a comprehensive statutory regime under the DPDP Act. It further evaluates the key provisions of the Act, the establishment of the Data Protection Authority, and potential constitutional conflicts arising from state surveillance, data localization, and national security exceptions. Through a doctrinal and analytical lens, the paper also compares India's data protection landscape with international frameworks such as the EU's GDPR and OECD guidelines.

Ultimately, the paper argues that the success and legitimacy of the DPDP Act will hinge on its judicial interpretation—particularly how courts balance privacy rights with competing interests of the state and commercial stakeholders. The judiciary's continued vigilance in enforcing privacy norms, scrutinizing exemptions, and safeguarding constitutional values will be vital to ensuring a rights-based approach to data protection in India's digital future.

Introduction

The increasing reliance on digital technologies and the widespread collection and processing of personal data have highlighted the need for stringent legal frameworks that protect individuals' privacy. The Digital Personal Data Protection (DPDP) Act, 2023, represents a significant legal step in India toward safeguarding personal data in the digital realm. As digital technologies evolve rapidly, the act addresses concerns regarding the privacy of individuals, particularly in the context of the growing digital economy, government surveillance, and corporate data collection. The Indian judiciary, through various constitutional pronouncements, has been instrumental in shaping the legal landscape of data protection, and its approach to the DPDP Act will significantly influence how it functions in practice.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

India's increasing digitization, coupled with the massive collection of personal data by private companies and government bodies, has raised significant concerns regarding individual privacy. Until the enactment of the DPDP Act, India's data protection framework was limited, relying mainly on provisions in the Information Technology Act, 2000 (IT Act). The IT Act addressed cybercrimes and data security but failed to provide a robust mechanism for data protection. As digital platforms like e-commerce, social media, and digital payments expanded, the risk of personal data misuse and breaches grew, leading to calls for comprehensive data protection legislation.

The Indian judiciary played a crucial role in raising awareness about privacy rights through landmark cases. The K.S. Puttaswamy v. Union of India judgment (2017) laid the groundwork for a robust data protection regime. The Supreme Court ruled that the Right to Privacy is a fundamental right under Article 21 of the Indian Constitution. This judgment not only affirmed the right to privacy but also recognized personal data protection as a component of privacy, thereby catalyzing the need for specific legislation. The judicial interpretation of privacy as a fundamental right set the stage for a formal legislative response, eventually leading to the drafting of the Personal Data Protection Bill, 2019, which was later amended and became the DPDP Act, 2023.[1008]

The judiciary's role in shaping the DPDP Act cannot be understated. The Indian legal system has historically played a critical role in interpreting and expanding the scope of fundamental rights. The Supreme Court has been at the forefront of advancing privacy rights, and its decisions in privacy-related matters continue to influence the trajectory of the country's data protection laws.

The Puttaswamy judgment provided the constitutional framework that ultimately informed the Personal Data Protection Bill, 2019, and the subsequent DPDP Act, 2023. One of the most significant aspects of the judgment was its recognition of the need for a legislative framework to regulate the collection and use of personal data by both government and private entities. The court's opinion called for the balancing of privacy with other competing interests, such as national security, public order, and the economic benefits of data processing. The judgment highlighted the necessity for clear guidelines on data processing, including consent, transparency, and accountability, which the DPDP Act seeks to address.[1009]

Key Provisions of the DPDP Act, 2023

The DPDP Act, 2023, aims to provide a comprehensive data protection regime that aligns with global data protection standards, such as the General Data Protection Regulation (GDPR) of the European Union. It establishes a legal framework for the protection of digital personal data and addresses issues related to data consent, processing, breach notification, and penalties for non-compliance. The law's provisions require data fiduciaries (entities that collect and process personal data) to seek the explicit consent of individuals before processing their data, with limited exceptions, such as for national security or public interest.

One of the key features of the DPDP Act is the establishment of a Data Protection Authority (DPA), which will regulate the implementation of the law and ensure compliance. The DPA will be tasked with investigating complaints, adjudicating disputes, and imposing penalties for violations of the law. The Act also provides individuals with several rights, including the right to access, rectify, and erase their personal data. It recognizes the importance of cross-border data transfers and introduces provisions to ensure that data flows are compliant with Indian laws.

However, the DPDP Act also raises concerns regarding its provisions on data localization and government surveillance. The law requires data

[1008] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1. (Accessed March 2, 2023 from https://www.scjudgments.in).

[1009] Government of India, Personal Data Protection Bill, 2019. (Accessed March 2, 2023 from https://www.indiabill.gov.in).

fiduciaries to store certain data within India, potentially raising issues related to international business operations and global data flows. Critics argue that the Act could enable government overreach in the form of surveillance, as it provides broad exemptions for data processing in the interests of national security, law enforcement, and public order. These provisions have led to debates about the fine line between safeguarding national security and protecting individual privacy.[1010]

Judicial Scrutiny of the DPDP Act, 2023

The judicial approach to the DPDP Act will be critical in interpreting its provisions and ensuring that the Act is applied in a way that protects citizens' privacy while balancing the interests of the state and businesses. In particular, the right to privacy guaranteed by the Constitution will continue to serve as a guiding principle in the interpretation of the DPDP Act. The Supreme Court and High Courts will play an essential role in resolving conflicts that arise between data subject rights, business interests, and state surveillance.

Future court review of the Act's data localization as well as national security provisions is probably in the works. It will be left to the Supreme Court to decide whether the Act's exclusions for government monitoring align with people's fundamental right to privacy. The judiciary must determine whether such acts are appropriate and follow the necessity and proportionality grounds outlined in the Puttaswamy ruling, for instance, if the government wants access to personal data for security reasons.

In addition, it is expected that the Act's establishment of the Data Protection Authority (DPA) would be tested in court for its efficacy and impartiality in enforcing data protection laws. The legal review of DPA's decisions and its power to impose penalties will determine the Act's effectiveness. Furthermore, the courts will have to decide whether the act's right to be forgotten is implemented, particularly in cases where data subjects ask for the deletion of their personal data.[1011]

The success of India's data protection system would be greatly influenced by the judiciary's handling of the DPDP Act, 2023. Although the Act represents a major advancement in India's efforts to protect personal data, how well the courts apply and interpret its provisions will determine how effective it is in practice. The judiciary must preserve people's privacy while taking into account the state's and corporations' legitimate interests as India transitions to a more data-driven future. In order to ensure that the nation's digital economy develops in a safe and privacy-conscious way, the judicial review of the DPDP Act would be crucial in finding the ideal balance among protection of data, privacy rights, as well as national security considerations.[1012]

The ITA was passed in order to provide a thorough regulatory framework for online sales. Sections 69 and 75 of the Act are relevant when discussing the right to privacy on the web. Similar to Section 5(2) of the Indian Telegraph Act of 1885, Section 69 gives the Controller the authority to order any government agency to intercept any data sent via a computer resource and mandates that users reveal their encryption keys or risk a maximum seven-year jail sentence.On the other hand, Section 72 is the only specific clause in the act that deals with privacy and confidentiality violations. It states that anyone who divulges the information contained in any electronic record, etc., without the owner's authorization faces up to two years in prison, a fine of up to one lakh rupees, or both.

However, both the provisions within the Information Technology Act (2000) deal specifically with the powers of the govt in reference to the privacy of people . From an

[1010] Government of India, Digital Personal Data Protection Act, 2023. (Accessed March 2, 2023 from https://www.meity.gov.in).

[1011] K.S. Puttaswamy (Retd.) vs. Union of India, (2017) 10 SCC 1. (Accessed March 2, 2023 from https://www.scjudgments.in).

[1012] Digital Personal Data Protection Act, 2023, Government of India (retrieved March 2, 2023 from https://www.meity.gov.in)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 5 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

understanding of the Indian legal scenarios, it are often concluded that there exists no Indian legislation that covers the protection of rights of privacy, which may be interpreted within the realm of transactions between individuals and corporations or between two individuals over the web.

Privacy as a Fundamental Right in India

"As already discussed Article 21 of the Constitution of India states that No person shall be deprived of his life or personal liberty except according to procedure established by law. The right to life enshrined in Article 21 has been liberally interpreted so as to mean something more than mere survival and mere existence or animal existence. It therefore includes all those aspects of life which makes a man's life more meaningful, complete and worth living and right to privacy is one such right. The first time this topic was ever raised was in the case of ***Kharak Singh v. State of UP***[1013]***,*** where the Supreme Court held that Regulation 236 of UP Police regulation was unconstitutional as it clashed with Article 21 of the Constitution. It was held by the Court that the right to privacy is a part of right to protection of life and personal liberty. Here, the Court had equated privacy to personal liberty."

"In ***Govind v. State of Madhya Pradesh***[1014], Mathew, J. accepted the right to privacy as an emanation from Art. 19(a), (d) and 21, but right to privacy is not absolute right. Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right to privacy is itself a fundamental right, the fundamental right must be subject to restriction on the basis of compelling public interest. Surveillance by domiciliary visits need not always be an unreasonable encroachment on the privacy of a person owing to the character and antecedents of the person subjected to surveillance as also the objects and the limitation under which the surveillance is made. The right to privacy deals with 'persons not places'."

"In ***Smt. Maneka Gandhi v. Union of India & Anr.,(1978)***[1015] in this case SC 7 Judge Bench said 'personal liberty' in article 21 covers a variety of rights & some have status of fundamental rights and given additional protection u/a 19. Triple Test for any law interfering with personal liberty: (1) It must prescribe a procedure; (2) the procedure must withstand the test of one or more of the fundamental rights conferred u/a 19 which may be applicable in a given situation and (3) It must withstand test of Article 14. The law and procedure authorising interference with personal liberty and right of privacy must also be right just and fair and not arbitrary, fanciful or oppressive."

"In ***Naz Foundation Case (2009)***[1016] Delhi HC gave the landmark decision on consensual homosexuality. In this case S. 377 IPC and Articles 14, 19 & 21 were examined. Right to privacy held to protect a private space in which man may become and remain himself. It was said individuals need a place of sanctuary where they can be free from societal control- where individuals can drop the mask, desist for a while from projecting on the world the image they want to be accepted as themselves, an image that may reflect the values of their peers rather than the realities of their nature."

Right To Privacy-Permissible Restriction

"Intrusion into privacy may be by- (1) Legislative Provision (2) Administrative/Executive order (3) Judicial Orders. Legislative intrusion must be tested on the touchstone of reasonableness as guaranteed by the Constitution and for that purpose the Court can go into proportionality of the intrusion vis-à-vis the purpose sought to be achieved. (2) So far as administrative or executive action is concerned it has to be reasonable having regard to the facts and circumstances of the case. (3) As to judicial

[1013] AIR 1964(1) SCR 332
[1014] (1975) 2 SCC 148
[1015] *1978* SCR (2) 621
[1016] *Naz Foundation* v Government of NCT of Delhi and Others ((*2009*) 111 DRJ 1)

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 5 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

warrants, the Court must have sufficient reason to believe that the search or seizure is warranted and it must keep in mind the extent of search or seizure necessary for protection of the particular State interest. In addition, as stated earlier, common law did recognise rare exceptions for conduct of warrantless searches could be conducted but these had to be in good faith, intended to preserve evidence or intended to prevent sudden anger to person or property."

The Privacy Bill, 2011

The bill says, 'every individual shall have a right to his privacy — confidentiality of communication made to, or, by him — including his personal correspondence, telephone conversations, telegraph messages, postal, electronic mail and other modes of communication; confidentiality of his private or his family life; protection of his honour and good name; protection from search, detention or exposure of lawful communication between and among individuals; privacy from surveillance; confidentiality of his banking and financial transactions, medical and legal information and protection of data relating to individual.

The bill gives protection from a citizen's identity theft, including criminal identity theft (posing as another person when apprehended for a crime), financial identify theft (using another's identity to obtain credit, goods and services), etc.

The bill prohibits interception of communications except in certain cases with approval of Secretary-level officer. It mandates destruction of interception of the material within two months of discontinuance of interception.

The bill provides for constitution of a Central Communication Interception Review Committee to examine and review the interception orders passed and is empowered to render a finding that such interception contravened Section 5 of the Indian Telegraphs Act and that the intercepted material should be destroyed forthwith. It also prohibits surveillance either by following a person or closed circuit television or other electronic or by any other mode, except in certain cases as per the specified procedure.

As per the bill, nobody who features a place of business in India but has data using equipment located in India, shall collect or processor use or disclose any data concerning individual to a person without consent of such individual.

The bill mandates the establishment of a knowledge Protection Authority of India, whose function is to watch development in processing and computer technology; to look at law and to guage its effect on data protection and to offer recommendations and to receive representations from members of the general public on any matter generally affecting data protection.

The Authority can investigate any data security breach and issue orders to safeguard the safety interests of affected individuals within the personal data that has or is probably going to possess been compromised by such breach.

The bill makes contravention of the provisions on interception an offence punishable with imprisonment for a term which will extend up to 5 years or with fine, which can reach Rs. 1 lakh or with both for every such interception. Similarly, disclosure of such information may be a punishable offence with imprisonment up to 3 years and a fine of up to Rs. 50,000, or both.

Further, it says any persons who obtain any record of data concerning a private from any officer of the govt or agency under false pretext shall be punishable with a fine of up to Rs. 5 Lacs.

Right to Privacy and Search and Seizure

The right of privacy on one hand and power of the State of search and seizure on the opposite hand has been the topic matter of judgments not only in India but also in other countries also. The Supreme Court mentioned American case laws under the Fourth Amendment to the US Constitution. The Court also mentioned

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 5 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Universal Declaration of Human Rights, European Convention of Human Rights, other treaties and constitutional provisions and held that the State cannot have unbridled right of search and seizure. especially, it acknowledged that each one public records could always be inspected but it'll not be hospitable Collector under the impugned amended Section 73 of the Indian Stamp Act, 1899 to direct the assembly of records held with banks. These records are copies of personal documents. The proper to privacy is to guard the documents which are with the banks. Unless there's reasonable cause or material to believe that such documents may cause a discovery of fraud such documents can't be inspected. The Court struck down S. 73 giving uncontrolled power to Collector to authorize a person to require notes or extracts from such documents. Even the principles framed under the Act didn't provide sufficient guidelines or safeguards on how this power might be exercised. The Supreme Court mentioned US judgments on this subject. It preferred to follow the minority view in Miller's case and took the view that majority decision was incorrect. It also mentioned various articles and comments which have taken the view that majority judgement was wrong the Court held that documents or copies thereof given to the bank will still remain confidential. the very fact that they're given to bank voluntarily won't mean that they cease to be private records as mentioned above.

Tapping of Telephone

Telephone tapping constitutes a significant invasion of an individual's right to privacy. Is it constitutionally permissible in India? If so, within what limits and subject to what safeguards?

The questions posed above have been fully considered by the Supreme Court in ***People's Union for Civil Liberties v. Union of India***[1017]. In this case Public Interest Litigation was filed protesting rampant instances of phone tapping of politician's phones by CBI. The court ruled that 'telephone conversation is an important facet of a man's private life'. The right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as 'right to privacy'. So, tapping of telephone is a serious invasion of privacy. This means that telephone tapping would infract Article 21 unless it is permitted under the procedure established by law. The procedure has to be 'just, fair and reasonable'.

The Court laid down exhaustive guidelines to regulate the discretion vested in the State under Section 5 of the Indian Telegraph Act for the purpose of telephone tapping and interception of other messages so as to safeguard public interest against arbitrary and unlawful exercise of power by the Government. Section 5(2) of the Act permits the interception of messages in accordance with the provisions of the Act."Occurrence of any public emergency" or "in interest of public safety" are prerequisites for the application of provisions under section 5(2) of the Act; in the absence of either, the authorities lack the authority to exercise their authority under the aforementioned legislation. A public emergency, according to the Court, is a sudden condition or state of affairs that affects the general public and necessitates quick action. The phrase "public safety" refers to a situation in which the general populace is in great danger or peril.

The Court ruled that in the absence of either of these two requirements, the Central Government, State Governments, or authorized officers cannot use telephone tapping, even if they are satisfied that doing so is required or practical for maintaining the nation's integrity and sovereignty.

In other words, unless a public emergency has occurred or the public interest in public safety demands it, the Central Government cannot intercept messages or use telephone tapping, even if it is convinced that doing so is necessary or timely to protect the nation's sovereignty or integrity, the security of the State, friendly

[1017] AIR 1997 SC 568

relations with other nations, public order, or to prevent incitements to commit crimes.

The Court established the following procedural protections for the use of authority under Section 5(2) of the Indian Telegraph Act: ·

Only the house secretary of the federal government or the state governments may typically issue an order for telephone tapping. A politician from the Central Government's home department, and therefore the State Governments, who has a position higher than joint secretary, could also be given the facility in an emergency.

·Within a week of the order being passed, a copy of the order must be provided to the Review Committee.

· The order will no longer be in effect after two months—unless it is renewed. If the governing body deems it essential to extend the order in accordance with Section 5(2) of the Act, it may review prior to that time. The record of intercepted conversations, the amount of fabric to be disclosed, the number of people, and their identities must be kept up to date by the authority making the order.

The use of intercepted material will be restricted to the bare minimum required by Section 5(2) of the Act.

· The Review Committee will independently, within two months, look into whether or not a relevant order under Section 5(2) of the Act has been issued.

· Should the Review Committee find that Section 5(2) of the Act has been violated, the order will be revoked. Additionally, it has the ability to order the destruction of the intercepted material's duplicates.
· Should the Review Committee conclude after conducting an investigation that there has been no violation of the applicable Act provision, it will document the findings accordingly.

The Court pointed out that as highly advanced communication technology advances, the right to have an uninterrupted conversation in one's home or place of business is becoming more and more susceptible to misuse. Given this, the Court's decision that establishes comprehensive rules for the use of authority under the applicable Act is both historic and pertinent.

Divorce Petition:

By listening in on his wife's conversations with people who want to produce in court, the husband violates her right to privacy under Article 21.

In ***Rayala M. Bhuvneswari v. Nagaphomender Rayala***[1018]the petitioner filed for divorce from his wife and wanted to provide a hard disc containing a recording of his wife's conversations with other people in the United States as evidence. Parts of the chat were refuted by her. The Court ruled that the husband's illegal tapping of his wife's conversations with others without her knowledge violated her right to privacy under article 21 of the Constitution. Even if they are factual, these conversations cannot be used as proof. The woman cannot be made to take a voice test without her will and then have the expert compare the parts of her voice that she denied with the ones that she admitted.The Court noted that the foundation of marriage is the integrity of the husband and wife's relationship. Without her knowledge, the spouse was recording her phone conversations with her parents and friends in India. This clearly violates the wife's right to privacy. The concept of marriage itself becomes unnecessary if a husband is like this and doesn't trust his wife, not even when it comes to her interactions with her parents.

Prisoner's Privacy Rights

Even incarcerated convicted individuals are protected under Article 21. The convicted are not denied any of their other fundamental rights only because they were found guilty. The right to travel freely across India is one of the fundamental liberties that a convicted criminal

[1018] AIR 2008 AP 98

may lose after being placed in jail. However, a convicted individual is entitled to the priceless right protected by Article 21 and cannot be deprived of his life or personal freedom until a legally mandated process is followed.

In the case of ***R. Rajagopal vs. State of T.N***[1019] also known popularly as the Auto Shankar Case, the issue of the right to be left alone once more came up. An inmate wrote an autobiography while incarcerated, detailing the circumstances inside and the interactions between inmates and a number of IAS and IPS officers. He had given his wife the memoirs so she could publish it in a specific magazine. The publishing was constrained in a number of ways, though, and it raised the question of whether anyone, especially those incarcerated, has the right to privacy

Conflict Between: Right To Information & Right To Privacy

The right to privacy is not specifically recognized by the Indian Constitution. However, following the *Kharak Singh v. State of U.P.* decision, the Supreme Court acknowledged for the first time the Constitution's implied right to privacy under Article 21. The Court ruled that although the right to privacy is a fundamental component of the right to life, it nonetheless exists in a murky area in the absence of unambiguous legislation. The opinion was founded on the finding that a basic right must be directly and visibly violated, and that a watch being kept on the suspect's movements did not violate the freedom of speech and expression protected by u/a 19(1)(a).

Indu Jain v. Forbes Incorporated[1020]**, 21 (2007)**

In this case Indu Jain filed a complaint with the courts to prohibit Forbes magazine from including her family under the Forbes List of Indian Billionaires. The publishing was permitted after the court decided against Indu Jain. Following a thorough analysis of the relevant literature, the Court identified the following principles:

The general public's interest in the published topic must be purely purely speculative. Public officials and other public figures have a significant impact on social order. They must have access to mass media communication in order to challenge criticism of their actions and opinions as well as to influence policy. The freedom of the press includes the ability to freely discuss public individuals' involvement in topics and events because citizens have a legitimate and significant interest in their behavior. ***R. Rajagopal & Anr. Vs. State of Tamil Nadu & Others Para 18***[1021].

A private's right to privacy may also be forfeited by him by explicit or implicit assent, or by a pattern of behavior that contradicts its claims. Such an inference could also be drawn from the participants' actions and, consequently, the situation at hand.

In the facts noticed above, in my view the plaintiff has did not figure out a case that publication effected by the defendants would be covered within the protection which is afforded to a person's right to privacy.

The principles laid down above clarify variety of issues regarding the proper to privacy and therefore the invasion of it by individuals within the Press. It says that court has got to balance the rights of the person whose privacy has been invaded against the liberty of press so therefore the right of public to disclosure of newsworthy information and in doing therefore the court has got to balance the 'proportionality of interfering with one right against the proportionality of impact by infraction of the other'.

However, the court determined in the Bharat Shanti Lal Shah matter that a statute can permit interception between two people even if doing so immediately violates their right to privacy, provided that the process for such a violation is straightforward, reasonable, and not capricious or burdensome. It has been observed that any

[1019] 1995 AIR 264
[1020] (2007) ILR 8 Del 9
[1021] (1994) 6 SCC 632

action claimed within the relational type of privacy must, first and foremost, be intimate and private in nature, and second, it must be compliant with the law.

Justice K.S. Puttaswamy V. Union Of India And Ors[1022]

Law cannot remain static. Various changes in the political, economic and social life of individuals demand the law to be dynamic. The economic theory of 'laissez faire' gained popularity in the 18th and the 19th centuary. This theory implied no government interference in commercial transactions. It gave monopoly status to the enterprises to act independently without any governmental interference. These theories can be regarded as one or the other form of right to privacy. Louis Brandeis and Samuel Warren first mentioned about privacy and the issues surrounding it in an article published in the Harvard Law Review dated December 16, 1860. The article took into consideration a broad look into a man's spiritual and intellectual behavior and concluded that right to privacy is a facet of right to life.

The recent ruling by the Supreme Court of India that the right to privacy is a fundamental right caused quite a stir. Amidst numerous disputes about the aforementioned right, privacy was ultimately deemed a basic right, enshrined in Article 21 of the Indian Constitution that protects the right to life. At first, there were sector-specific privacy rules in the United States of America. Later on, it evolved and took on several shapes. Given how information technology is being used more and more in practically every industry, it is imperative that this right be recognized. In order to preserve the privacy of the general public, Hessen, a German state, was the first to pass data protection legislation in 1970. Since then, at least 40 nations have passed legislation doing just that.

Surveillance and Privacy

A person is kept under surveillance in order that his/her activities might be traced which the person doesn't commit any longer crimes. This undoubtedly calls into question the violation of that individual's right to privacy. As was previously said, Kharak Singh's case was where the issue initially arose. However, the greater public interest cannot be disregarded in order to protect one individual's right to privacy. Several factors should be considered before placing someone under surveillance, including:

- The Criminal background of the person. Whether the person has actually committed such crimes which require keeping him/her under surveillance.
- The frequency of the person committing crime i.e. whether he/she commits crime repeatedly at frequent intervals or not.
- The level of crime committed i.e. it is of such heinous nature for the security of public it is necessary to trace the activities of the person.

In India, the government's surveillance operations are not governed by a single comprehensive law. Data is transported to various agencies around the nation on a daily basis, and the number of cyberattacks is rising, which eventually makes the public perceive a threat. The implementation of the National Intelligence Grid resulted from the height of counterterrorism efforts following the 2008 Mumbai bombings. The grid facilitates information sharing among India's 22 Central Intelligence Agencies. The Crime and Criminal Tracking Network System (CCTNS), which permits information exchange between various police stations and allows one police station to access data kept on the servers of other police stations, must also be emphasized.

All of these commonplace behaviors necessitate strict legislation to protect people's privacy. The right to privacy cannot be distinguished, and it cannot be argued that a person's private need not be preserved, especially if they have committed a crime. Therefore, Justice Harlan's "reasonable expectation of privacy test" contains the solution to the current situation. According to

[1022] AIR 2017 SC 4161

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 5 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

this criteria, an individual's privacy can never be infringed upon if they have a legitimate expectation of privacy in that particular location. One example of such a location is frequently a person's residence. One of the requirements for this is that society must acknowledge the expectation of privacy in such a place.

The Indian Computer Emergency Response Team (CERT-In) is another government agency that conducts surveillance. Although it isn't exactly the government's only surveillance agency, it strives to ensure cyber security. It has its roots in the Information Technology Act of 2008 and only becomes relevant when an attack is launched against an Indian server by a foreign entity or person. In addition, the Indian Telegraph Act places limitations on the government's ability to undertake surveillance by specifying the conditions under which it can do so. This has the ability to stop arbitrary invasions of privacy.As a result, it is frequently determined that, even while there are some situations in which laws governing monitoring are in place, specific laws must be passed once privacy has been deemed a fundamental right. The President has the sole authority to authorize monitoring in nations such as the United States, and this authority may even be granted following a writ. The Regulation of Investigatory Powers Act, 2000 is a piece of particular legislation in the United Kingdom that establishes guidelines for surveillance regulation.

Most of the days, surveillance is discussed on a national level only. However, it must be noted that there with the growing use of data technology, mass surveillance instances have also increased. However, thanks to the shortage of any international convention on mass surveillance, the countries feel free to carry out such mass surveillance activities on their own free will. This ultimately violates the privacy of individuals. This view is based on the Lotus Approach specified by International court of Justice wherein the Court expressly said that whenever there is no international legislation dealing with any matter, the State is free to choose their own actions and carry out the same. This is view has also given rise to instances of mass surveillance which ultimately violates privacy.

Private Space and Homosexuality

Same-sex marriages are no longer illegal in more than 30 nations, including Canada, the Netherlands, Ireland, and many more. Sexual activity that violates the natural order is punishable under Section 377 of the Indian Penal Code. The phrase "against the order of nature," which is used in the aforementioned section, encompasses the Lesbian, Gay, Bisexual, and Transgender (LGBT) community. This suggests that in India, having sex with someone from this community would be illegal. Some of the instances of being-

A truck driver who twice engaged in sodomy with a boy was disciplined. The driver was imprisoned and fined by the Gujarat High Court.[1023] Semen released from the victim's mouth would likewise be considered unnatural sexual activity.[1024].

Therefore, the nation punishes all kinds of unnatural offenses. But once the right to privacy was declared a fundamental right, the question that arises is: How could a private action like "unnatural sex" be punished when privacy is a basic right? After establishing privacy as a basic right, India urgently needs to legalize homosexuality. Law in itself cannot be contradictory, otherwise how will it maintain social order?

The topic of decriminalizing homosexuality was raised in 2009 when barrister Mr. Anand Grover filed a writ suit in the Delhi High Court, claiming that Section 377 of the IPC violated multiple parts of the Indian Constitution and deserved to be repealed. The petition was submitted by an NGO called the Naz Foundation. The Delhi High Court decriminalized homosexuality. The primary issue raised by the Supreme Court's

[1023] Chiranjit Singh v. State of Himachal Pradesh Cr Lj 1986 Guj HC 173 (Gujarat High Court).
[1024] Basantlal v. State AIR 1968 Guj HC 252. (Gujarat High Court).

subsequent hearing on a challenge to this decision was the constitutionality of the aforementioned section. But the Apex court overturned the judgment, ruling that the aforementioned portion is not unlawful. It is not gender-based discrimination. It imposes sanctions solely on the basis of an individual's actions.[1025]

A committee must be established by the government and the Supreme Court to look at the rising number of same-sex couples in the nation. The 2014 ruling by the Naz Foundation, which declared privacy to be a fundamental right, unquestionably needs to be reviewed. Even if it is unnatural, two people having private, consensual sex shouldn't be punished. Section 377 of the IPC should be repealed, according to the 172nd Law Report. It might not be brought up in this instance that marriage is primarily for the purpose of having children. Israel and other nations have legalized gay surrogacy. This would therefore not be a significant problem.

Privacy and Aadhar

The primary cause of the privacy invasion case was the Indian government's request for residents' biometric information in order to issue Aadhar cards. All citizens are required to have an Aadhar card under the Aadhar plan; otherwise, they may face difficulties opening bank accounts, paying taxes, and other related tasks. The main argument was that since the Aadhar Act does not require enrollment, the aforementioned plan does not violate anyone's rights because everyone provides their biometric information willingly.

It must be acknowledged that the Indian government undoubtedly offers the nation's impoverished a range of social security advantages. A citizen would not be eligible for this benefit if they did not have an Aadhar card. In the end, this would deny them the advantages and produce many irrational groups of citizens, which would again be against Article 14 of the Indian Constitution, which guarantees the right to equality.

The fact that there is unquestionably evidence of undue influence here is another factor supporting the scheme's legitimacy. The idea that what cannot be done directly cannot be done indirectly is the foundation of the notion of colorable legislation. The Aadhar Act is unquestionably a type of colorable law in which the government surreptitiously and indirectly exerts undue control over particular societal segments. Food and shelter would undoubtedly be the first things a citizen would select if they were to choose between privacy and social welfare programs.

Another problem with the aforementioned issue is that the government did not enact strict legislation to protect residents' personal information even after the implementation of such a program. Even if the IT Act has undergone multiple amendments to strengthen data privacy regulations, stricter legislation should to be introduced in order to implement the Aadhar Scheme. The government must be legally obligated to disclose the rationale behind data acquisition and assume responsibility for data security.

One of the solutions to prevent such unauthorized leak of personal data can be by allowing anonymous access to services and anonymous surfing of internet. However, this can also create many problems and would give rise to more cyber crimes. It is essential that privacy be recognized as a fundamental right in light of various international accords, including Article 8 in the European Convention along with Article 12 of the UN Declaration of Human Rights. The Indian Supreme Court rendered a correct ruling, and strict data protection regulations must be put into effect. Following the ruling, the Parliament must pass the privacy measure that is now pending.

Privacy as a Horizontal Right

It is crucial to remember that the right to privacy has been acknowledged as a standard

[1025] Suresh Kumar Kaushal v. Naz Foundation AIR 2014 SC 563 (Supreme Court of India).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 5 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

law right for a considerable amount of time. In fact, the Union of India has stated that privacy ought to only be recognized as a standard law right. As a result, it had been used as a component of tort law between private parties long before the Puttaswamy issues gained attention. However, whether or whether privacy might be a basic right within the Indian Constitution was the main issue in Puttaswamy. The judges gave an affirmative response to this.

According to a nine-judge Supreme Court panel, Indians have a fundamental right to privacy, which is protected by Article 21 of the Indian Constitution since it is essential to life and liberty.

The bench comprised judge Khehar and Justices J. Chelameswar, S.A. Bobde, R.K. Agrawal, Rohinton Nariman, A.M. Sapre, D.Y. Chandrachud, Sanjay Kishan Kaul and S. Abdul Nazeer.

In its 547-page decision,By reversing decisions related to the M.P. Sharma matter from 1958 and, consequently, the Kharak Singh case from 1961, which both argued that the Indian constitution failed to safeguard the right to privacy, the Supreme Court affirmed privacy as a basic right.

Indian Legislation on Social Media Privacy and Data Protection

Laws related to social media and privacy in India are clearly insufficient. The Indian judiciary and legislature have proved to be far behind expectations when it comes to the framing of laws in this arena. Some rules and legislations have been issued, those too are primarily related to defamation.

Now let's come to the Information and Technology Act, 2000. The concept of privacy in this act is comprehended in a very liberal and traditional sense. The act of knowingly sending pictures of a person's private parts, without his permission, then Section 66E of this act is violated. Social media finds only a mention in Section 79 of this act. This section clarifies that if any person posts or uploads anything derogatory to some other, then the medium on which it is posted, that is Twitter, Facebook etc, is not to be held liable for the acts of such person. Beyond this, nothing is mentioned in the whole article with regard to social media. Let us understand this by a simple example- If X, a Facebook user posts something derogatory to Y, another Facebook user, then Facebook is not to be blamed for X's act.

This concept has however evolved with time, in the case of ***Shreya Singhal***[1026], it was held that it is Facebook's duty to remove any material posted by them which is objectionable. This has to be done by Facebook, applying its discretion, after complaints regarding the same are received.

Next, let's learn about the recent Whatsapp-Facebook Privacy Case or ***Karmanya Singh v. Union of India***[1027]. Constitutional rights were meant to deal primarily with the relationship between the state and individuals. However, this concept has seen a marked change due to the boom of privatisation in India. Private companies have taken up many functions which are traditionally associated with the state. Our Constitution makers, however, had framed laws according to the situation of the country which was prevailing at that time.

Due to these changed conditions, these private actors when performing state-like actions are subjected to the same Constitutional scrutiny. In the case at hand, the contract between two social networking sites, Whatsapp and Facebook was challenged, both private parties, invoking the above-mentioned ideology.

With the debut of social media, a new term of Internet privacy has come into lime-light. Data protection and Internet privacy are not specifically covered by any laws. However, the privacy lock granted by Article 21 of our constitution is insufficient to adequately protect the data. However in the year 2000, legislature made effort to embrace social media privacy issues and currently India's most

[1026] Shreya Singhal v. Union of India, AIR 2015 SC 1523
[1027] Karmanya Singh Sareen v. UOI, 233 (2016) DLT 436.

comprehensive legal provisions that speaks of privacy on the Internet is the Information Technology Act, 2000. Even though it cannot completely safeguard the privacy, it can dilute it to an extent. Provisions that clearly protect user privacy include Section 43, 66, 66F and 67 of the Information Technology Act, 2000 and also the rules of the Act.

Privacy in Electronic Media

In India, the IT Act largely regulates the monitoring, decoding, intercepting, and information gathering of digital communications. Section 69 of the IT Act, in particular, gives the Central Government and State Governments the authority to give directives for the monitoring, intercepting, and decryption of any information sent, received, or stored via the use of computers for the purposes of maintaining public order, defense, security, good relations with other countries, the sovereignty and integrity of India, averting incitement from committing any of the previously mentioned crimes, and looking into any offense.

With regard to the concern of Intermediaries violating the right to privacy on the internet, India has adopted the Safe Harbor Model. Under this model, the liability of an intermediary with respect to illegal or offensive content hosted by it is dependent upon the role played by the intermediary in distributing such content. India adopted the conditional safe harbor approach in 2008 by amending the Information Technology Act, 2000 after the Avnish Bajaj case[1028].

Conclusion

Regarding the protection and privacy of data, India's legal environment has seen a substantial change with the passage of the Digital Protection of Personal Data (DPDP) Act, 2023. Strong data protection regulations are now essential to protecting people's privacy throughout the digital era due to the rapid advancement of technology. The Court's focus on striking a balance between privacy, security, along with state interests is reflected in the approach it takes to this Act, particularly in light of earlier constitutional rulings and legal precedents. This law's passage and judicial review were made possible by the Supreme Court's engagement in privacy-related issues, particularly through the seminal K.S. Puttaswamy (Retd.) vs. Union of India decision.

A major turning point in the official recognition of privacy as a basic right under Article 21 of Indian Constitution was the Puttaswamy ruling in 2017. The Supreme Court decided that the constitutionally given right to privacy includes the protection of personal data. In addition to establishing privacy as a basic right, this historic decision allowed for the formation of the Srikrishna Committee, whose mission was to draft India's first data protection legislation. The Bill for Protecting Personal Data, 2019 was created as a direct result of the Court's ruling, which aimed to provide a statutory framework for securing personal data.

The DPDP Act, 2023 is inspired by the Puttaswamy verdict and worldwide data protection norms, particularly the General Privacy Regulation (GDPR) within the European Union. Protecting digital personal data, operating it lawfully, and upholding individuals' rights over their data are all highly valued under the law's provisions. The Data Protection Authority (DPA), established under the Act, was tasked with monitoring adherence and addressing grievances. However, there has been criticism of the Act's scope of governmental jurisdiction, particularly in sight of data localization along with the potential for state surveillance. The legal approach would most likely continue to assess the equilibrium between governmental interests as well as individual privacy to ensure that any such authority does not infringe upon people's fundamental rights.

One key aspect that will continue to evolve is how the judiciary interprets the rights of data subjects under the DPDP Act. The Act grants

[1028] Avnish Bajaj vs State (N.C.T.) Of Delhi, (2005) 3 CompLJ 364 Del

individuals several rights, including the right to access, correction, and erasure of personal data. However, the Act also provides several exemptions under national security, public order, and sovereignty considerations, which could create potential conflicts between individual rights and state interests. The judiciary will be tasked with interpreting these provisions in a way that ensures individuals' rights to privacy are upheld without compromising public safety or national security. The Court's prior stance in cases like Shreya Singhal v. Union of India (2015), which struck down overly broad provisions in the Information Technology Act (IT Act, 2000), has set a precedent that encourages caution when balancing freedom and regulation.

The judicial review of the DPDP Act will also likely extend to data breaches and the obligations of data fiduciaries under the law. As data breaches have become increasingly common, the role of the judiciary in enforcing penalties and ensuring accountability will be crucial to maintaining public trust in data protection mechanisms. Courts will need to evaluate how well the DPDP Act aligns with international standards on data protection while considering the nuances of India's socio-economic and political context.

In conclusion, the judicial approach to the DPDP Act, 2023 will be crucial in shaping the future of data protection in India. While the Act marks a positive step towards ensuring greater data privacy for citizens, its ultimate effectiveness will depend on how the judiciary interprets and applies its provisions, particularly regarding government powers, enforcement mechanisms, and individual rights. The judiciary's role will be essential in refining the law to strike the right balance between privacy, security, and freedom.