
INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

**THE RIGHT TO PRIVACY IN THE DIGITAL AGE: LEGAL
IMPLICATIONS AND CHALLENGES**- Dr. Kunal Shaktawat¹**Abstract:**

The right to privacy has faced several legal ramifications and difficulties in the digital age. This research attempts to offer insights into the complexities of privacy in the digital era by an extensive assessment of the literature and analysis of pertinent approaches. This study examines whether or not people's right to privacy is preserved in the digital era and what obstacles they must overcome to exercise that right. This study aims to determine people's awareness of the current legal framework and its implications, as well as to provide a concise explanation of the necessity of strict regulations protecting people's right to privacy. The study's findings make it abundantly evident that most of the participants are well aware of the right to privacy and how it affects an individual's right to privacy; however, the government must nonetheless enact laws that raise public awareness and protect citizens' rights in the digital age.

Keywords:

Privacy rights, Digital age, Legal implications, Privacy Protection, Data protection, Surveillance.

Introduction:

The digital revolution has completely changed how we engage, communicate, and do business. Technology presents previously unheard-of chances for creativity and connectedness, but it also poses serious issues with respect to private rights. Digital communications technology has permeated daily life, including the Internet, smartphones,

¹ Associate Professor in Law, Oriental University Indore (M.P.)

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

and gadgets with Wi-Fi capabilities. Innovations in communications technology have increased freedom of expression, enabled international discussion, and promoted democratic involvement by significantly enhancing access to information and real-time communication. These potent tools promise better enjoyment of human rights by magnifying the voices of human rights activists and giving them new means of documenting and exposing abuses. This introduction provides an overview of the key issues surrounding the right to privacy in the digital age, outlining the objective and scope of the research.

Indian Jurisprudence on Right to Privacy

Article 21 of the Indian Constitution offers that “*No person shall be deprived of his life or personal liberty except according to procedure established by law*”. The Supreme Court ruled on 24 August 2017 that the right to privacy is a fundamental right guaranteed by Part III of the Indian Constitution. This decision on the legislation and regulations will have far-reaching ramifications. New regulations will now be tested on the same parameters on which the laws that violate personal freedom are tested in accordance with Article 21 of the Indian Constitution. The right to privacy is now unambiguously accessible—its contours and boundaries are the issue that remains exceptional.

India has no extensive data protection and privacy legislation. The current laws and policies are of a sectoral nature in essence. As of now, in addition to other sectoral legislation, the appropriate regulations of the Information Technology Act, 2000 and its regulations govern the collection, processing and use of ‘private information’ and ‘delicate private data or information by a corporate body in India.

The Supreme Court first regarded whether the ‘right to privacy’ is a basic right in the case of *M. P. Sharma and Ors. v Satish Chandra, District Magistrate, Delhi and Ors.* where the warrant granted for search and seizure was questioned pursuant to Sections 94 and 96(1) of the Criminal Code of Procedure. The Supreme Court ruled that the search and seizure authority was not contrary to any constitutional provision. The Court also refused to recognize the right to privacy as a basic right guaranteed by India’s Constitution.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Thereafter, in the case of *Kharak Singh v State of Uttar Pradesh and Ors.* the Court regarded whether it would be an abuse of the right guaranteed under Article 21 of the Constitution of India to monitor an accused's home visits at night, thus raising the question of whether Article 21 included the right to privacy. The Supreme Court ruled that, in reality, such monitoring was contrary to Article 21. Moreover, the majority judges held that Article 21 did not expressly provide for a provision of privacy, and therefore the right to privacy could not be interpreted as a fundamental right.

Subsequently, in the case of *Gobind v State of M.P.* Police's right to housekeeping was questioned to be incompatible with the right to privacy enshrined in Article 21 of the Indian Constitution. The Supreme Court ruled that the laws of the police did not comply with the principle of private liberty and also acknowledged the right to privacy as a basic right guaranteed by the Indian Constitution, but supported the development of the right to privacy on a case-by-case basis and denied it as an absolute right.

This issue was once again raised before the Supreme Court in the case of *K. S. Puttaswamy (Retd.) v Union of India*, in that case, the Aadhaar Card Scheme was questioned on the ground that the collection and compilation of population and biometric information of citizens of the nation to be used for different reasons infringed the basic right to privacy enshrined in Article 21 of the Indian Constitution. Given the ambiguity surrounding the constitutional status of the right to privacy from previous judicial precedents, the Court referred the matter to a constitutional panel composed of nine (nine) judges.

The Supreme Court ruled that the right to privacy is inherent to the human element and the core of human dignity and is inseparable from it. Accordingly, privacy was kept to have both beneficial and negative content. The adverse content functions as an embargo on the State by intruding into a citizen's life and private freedom, and its beneficial content imposes a duty on the State to take all needed steps to safeguard the individual's privacy.

Therefore, the constitutional protection of privacy may give rise to two inter-related protection:

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

(i) Against the world at large, to be respected by all including the State: the right to choose what personal information is to be released into the public space.

(ii) Against the State: as necessary concomitant of democratic values, limited government and limitation on power of State.

As a consequence of this judgement, the right to privacy has become more than just common law and more solid and sacrosanct than any statutory right. Thus, an invasion of privacy must now be justified in the context of Article 21 of the Constitution on the grounds of a law stipulating a fair, just and sensible procedure.

Legislative Framework on the Right to Privacy

In light of escalating apprehensions over the privacy of individuals' data on social media, there arose a necessity for a resilient and all-encompassing legal framework to govern the data protection landscape and uphold the privacy rights established under Article 21. To protect people' data and privacy, the Indian Parliament adopted the highly anticipated 'Digital Personal Data Protection Act ("DPDPA") in August 2023 which represents a significant achievement as India's inaugural comprehensive legislation for data protection.

Prior to the current legislation, data privacy was partially protected under the Information Technology Act of 2000 and the Information Technology (Reasonable security practises and procedures and sensitive personal data or information) [SPDI] Rules of 2011, but these statutory provisions were deemed insufficient to adequately safeguard citizens' right to privacy.

The 'Digital Personal Data Protection Act 2023' outlines a structure for addressing digital personal data which preserves citizens' right to privacy while also embracing that the handling of such data is crucial for legitimate objectives, such as associated or incidental issues. The Act strongly entrusts data principals with control over their personal data, forbidding the storage and use of their data without express authorization—with the exception of some admissible situations in which an innovative concept known as "deemed consent" is incorporated. It also grants individuals the right to seek redress for grievances and the authority to designate individuals who will receive their data. It also gives individuals the

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

right to seek redress for grievances and the authority to decide who will obtain their data. In addition, the Act incorporates the "right to erasure," enabling users the ability to ask for an erasure of their personal information, offering them greater control over their online identity while also outlining commitments to entities identified as "data fiduciaries," which are in charge of gathering, archiving, and utilising digital personal data.

It also gives individuals the right to seek redressal for grievances and the authority to decide who will obtain their data. Moreover, the legislation incorporates the "right to erasure," granting users the capability to request the deletion of their personal information which enhances individuals' authority over their online identity. It is pertinent to note, however, that the Act does not explicitly incorporate the "right to be forgotten" as a separate provision, despite its acknowledgment as a crucial element within Article 21 under the aegis of the "Right to Privacy." The Act further highlights its commitment to responsible data management by outlining the responsibilities of organisations designated as "data fiduciaries," which are in charge of gathering, storing, and utilising digital personal data.

Therefore, by promoting transparency, fairness, and autonomy over personal data, the 'Digital Personal Data Protection Act 2023' fortifies the "right to privacy" guaranteed by Article 21 of the Indian Constitution

Social Media and Right to Privacy: How to strike a balance?

The internet has permeated every facet of existence, with modern technology skillfully weaving it all together. People establish connections with others and employ social media as a medium for communication. Furthermore, digital space functions as a platform for engaging in business transactions, procuring goods and services, accessing new information, and streamlining ordinary operations such as banking. With every internet transaction, the user unknowingly leaves electronic tracks that contain powerful means of information that provide knowledge about the user and their interests. In such an information age, which has been purported as "an era of ubiquitous dataveillance, or the systematic monitoring of citizen's communications or actions through the use of information technology", there exists a greater threat to the right to privacy of people as underscored in the Justice K.S. Puttaswamy v. Union of India.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

The consideration of incorporating the “right to privacy” into the Indian Constitution has been a subject of judicial scrutiny since its establishment, as it was never explicitly stated. The matter of recognising the “right to privacy” under Part III of the Constitution was raised during the M.P. Sharma v. Satish Chandra case, wherein the court decided not to make that determination. In the Kharak Singh v. State of U.P., although privacy was acknowledged, it was not yet deemed as an essential right, however, in PUCL vs Union of India, the court affirmed citizens' private interests and implemented legal safeguards to protect people's right to privacy against telephone tapping.

The landmark decision in Justice K.S. Puttaswamy v. Union of India, which revolved around Aadhaar, a government initiative providing a unique identification to Indian residents, confirmed the “right to privacy as a fundamental right” under Article 21. Article 21 safeguards the "Right to life and personal liberty" as part III of the Indian Constitution.

In the digital age of today, the “right to privacy” is significantly jeopardised by the growing dependence of individuals on the internet, particularly on social media platforms and such potential risk to private data becomes pronounced as individuals interact with technology. The watershed ruling of the nine-judge bench underscored concerns about the potential loss of privacy for individuals, cautioning against both state and non-state entities. This heightened risk arises from the increased interaction of individuals with technology, which has the capability to gather, archive, and mine information for the purpose of profiling individuals. On the one hand, social media portals give an effective platform for freely expressing oneself to an extensive demographic; however, on the other hand, they risk exposing the crucial confidential personal information of consumers.

The utilisation of "electronic tracks" by various social networking platforms to gather data from users for personalisation or targeted adverts poses an enormous threat to individual privacy. Moreover, extensive broadcasting of personal information on social media outlets is intrinsically injurious to individual privacy. Platforms like Facebook have frequently been embroiled in controversies regarding privacy and user security. Even during its nascent years,

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

it was observed that Facebook's algorithm was saving the incomplete posts and comments of the user even before it could be posted as "metadata." These concerns regarding user data were substantiated, particularly after the notable data privacy breach incident in the 'Cambridge Analytica Scandal,' in 2018, where the data and records of millions of people were harvested from Facebook by the data-harvesting enterprise Cambridge Analytica leading to infringement of "right to privacy" of the users.

Concerns over possible invasions of people' "right to privacy" have been prompted by recent privacy policy amendments made by X (formerly Twitter), which permit the collection of users' biometric data. In a similar vein, the Supreme Court of India is currently reviewing the privacy regulations that WhatsApp notified in 2016 and in 2021 after its takeover by Facebook in the case of Karmanya Singh Sareen & Anr. v. Union of India & Ors. The lawsuit seeks to uphold Indian residents' data and "right to privacy." According to WhatsApp's 2016 privacy policy, any consumer data published with the app will also be transmitted to Facebook, the parent organisation. The amended policy in 2021 stipulated that consumers would be unable to opt out of transferring data with Facebook if they intended to keep using the app; otherwise, their profile would be terminated. The present situation constitutes an imminent risk to the citizens' "right to privacy."

Another cause of concern regarding privacy is the long-term preservation of information on social networking services. For instance, Facebook's terms of use render it the liberty to archive private data indefinitely, establishing an irreversible extent of control over personally identifiable information. Consequently, even when a user wishes to cease using the social network, the data they provide remains beyond their control. Even the social media apps that are no longer operational in India, such as Tik-Tok can reportedly still continue to access data of Indian users from the app and are able to mine updated data and information of the individuals using the previously existing data which was stored on the app even after the app has been banned in India since 2020. This presents an enormous threat to the privacy of users' data, which nevertheless remains readily obtainable in the contemporary digital landscape and can be exploited by networking software to mine and profile updated information that relies on existing data. If unauthorised parties were to obtain such sensitive data, the implications may be catastrophic while jeopardising people's safety and causing a

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

grave infringement on their right to privacy as guaranteed by Article 21 of the Indian Constitution.

Current Issues and Legal Implications

The Supreme Court set a threefold necessity to interfere with fundamental rights by the state. While the State may intervene to safeguard the lawful interests of the State:

- (a) There must be a law in place to justify an infringement of privacy which is an express requirement of Article 21 of the Constitution;
- (b) The nature and content of the law imposing the limitation must fall within the reasonableness area prescribed by Article 14; and
- (c) The means taken by the legislatures.

Therefore, any regulations aimed at infringing an individual's right to privacy would have to satisfy the proportionality and reasonableness criterion. It will take a couple of years for jurisprudence to settle momentarily what constitutes sensible and proportionate state interference.

In contrast to today's consent-based model, it is often asserted that India should embrace rights-based information privacy models. The information controller is free to process, use and share the information with any third party under the consent-based model once the user's consent has been acquired. However, not many are conscious at the moment of approval of the real effects of indiscreet data sharing. The rights-based model, on the other side, enables consumers to have higher rights over their information while requiring the information controller to guarantee that users' privileges are not infringed. This results in the customers being more autonomous about their private information.

In the above judgments, the Supreme Court's judgment empowers Indian citizens to seek judicial relief in the event of infringement of their data privacy rights. This could have an

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

effect on India's tech companies privacy and security policies. Not only can consumers increase allegations based on torture, they can also invoke their fundamental right to privacy.

Concerns and difficulties

Nature of data protected by the Indian legislature

Since India lacks an extensive data protection mechanism, the primary act dealing with data protection is the IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011. Under the IT Act and the IT Rules, what is primarily intended to be protected are personal data and sensitive personal data or information, i.e. password-related information, financial information such as bank account or credit card or debit card or other payment tool details, physical, physiological and mental health condition, sexual orientation, medical records and history.

The information freely available in the public domain, however, is not considered within the scope of sensitive personal data or information. In addition, the regulations deal only with a corporate body collecting and disseminating data.

Who can collect the personal data

Rules 5 of the IT Rules stipulate that no corporate body or individual on its behalf shall gather delicate private data or information unless:

- (a) The information is obtained for a legitimate purpose related to the function or activity of the corporate body.
- (b) It is deemed appropriate to obtain such information for that purpose.

In addition, the person sharing the information must be made aware of the fact that the information is being collected, the purpose for which the information is being collected, the intended recipients of the information, the name and address of the agency collecting the information and the agency retaining the information.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Analysis

From above, it is obvious that the need for the hour is an extensive legislature governing the collection and dissemination of private information. There are no extensive laws governing the handling of private data that are not private data or information that is per se sensitive. WhatsApp Inc. has altered its privacy policy after being acquired by Facebook Inc. and users have been notified that users' WhatsApp account data will be shared with Facebook to enhance Facebook ads and product experiences, and users have been requested to agree to the updated terms for ongoing use of WhatsApp on or before September 25, 2016.

In perspective of this growth, Karmanya Singh Sareen and others submitted a written petition before the Delhi High Court arguing that removing the privacy of WhatsApp users' information and exchanging it with Facebook was in violation of users' basic freedoms guaranteed by Article 21 of the Constitution.

While deciding on the situation, the Delhi High Court instructed that if users opt to delete the WhatsApp account entirely, WhatsApp will delete user data entirely from its servers and refrain from exchanging user data with Facebook, and as far as users who choose to stay in WhatsApp are concerned, the current information/ data/ details of such users will not be communicated until 25 September 2016. The court also instructed the government to consider whether bringing messaging applications such as WhatsApp under some statutory legislative framework is viable.

Personal information protection is inextricably related to privacy, i.e. every person's right to enjoy his life and freedom without arbitrary interference with his private life, family, home or correspondence, etc. In contrast to the public, the term private must be grasped. Therefore, in the current obtrusive era of information technology, the right to be let alone and its security is highly essential. Since there is no single law that governs data protection in India comprehensively, it is necessary to derive the legal clauses regulating the same from multiple legislative acts.

Conclusion

As a cornerstone of individual freedom, privacy is a concept that is extremely essential for humanity. The right to privacy is rooted in human nature's unalienable rights and has historical relevance. In India, the acknowledgment of the right to privacy went through a

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

transforming journey before being affirmed as a fundamental right by a nine-judge Supreme Court bench in the \Justice K.S. Puttaswamy v. Union of India case.”

In the contemporary era, dominated by the pervasive influence of social media and the internet, has elevated the significance of privacy. Concerns have arisen due to the extensive storage of private information and the potential misuse of technology, particularly by malevolent actors. While social media creates a platform for global exchange and cooperation, it also exposes to individual privacy due to the extraction and utilisation of personal information.

The ever-evolving digital landscape necessitates a careful balance between privacy protection and technological progress and The ‘Digital Personal Data Protection Act 2023’ represents a significant step towards maintaining this balance and preserving the essence of personal liberty in the ever-expanding digital landscape.

Suggestions

Here are some suggestions for improving the right to privacy in India:

- **Protect personal data**

The government should ensure that personal and biometric data is protected and used only for the purpose it was collected for.

- **Pass a specific law**

Some say that the current legal framework is not enough to protect personal privacy rights. A specific law on privacy and data protection is needed.

- **Implement security measures**

Organizations should use encryption and anonymization to protect personal data.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

- Alert people to data breaches

Organizations should alert people if there is a data breach and give them access to their personal data.

- Conduct audits

Organizations should regularly audit their privacy procedures to understand what data they collect, how it's used, and where it's stored.

- Balance the right to privacy with the right to know

The government should not disclose personal information if it's not related to a public interest or if it would invade someone's privacy.

- Limit state action

State action can only limit the right to privacy if it has a legislative mandate, pursues a legitimate state objective, and is proportionate.

The government should ensure the proper mechanism to protect the personal and biometric data of individuals. It should use the data only for the purpose for which it is being collected and must refrain from using it for any surveillance purposes.

Reference

M. Gupta and S. Jha *"The Inclusion of Data Privacy in Antitrust Analysis"*,

A. Singh and U. Agarwal *"Privacy, National Security, and Government Interests:"*

A. Singh and A. Pathak *"Data Privacy in Covid-19 World"*

Anubhav Khamroi et Anjoy Shrimuktau, the curious case of right to privacy in India, O.P Jindal Global University

Right to privacy and data protection: Dr.Ankita Yadav

Right to privacy under Indian Law: Kiran Deshta

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Right to privacy – Arguing for the people: Vivek Sood, Bharat Law House

Right to privacy and freedom of Media: Dr.Lakhwinder Singh,Satyam Law International,
First Edition (1 January,2016)

Right to privacy: National and International Scenario ,Ramesh Kumar, Shandilya
Publications; First Edition (1 January 2019)



For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>