
INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

**THE RIGHT TO PRIVACY IN THE AGE OF DIGITAL TECHNOLOGY:
A STUDY WITH INDIAN CONTEXT**- Rohit Saini¹**ABSTRACT**

Every living thing on our planet enjoys the privilege of a feeling of self-insurance. Depending on their abilities, every human tries to protect himself from physical damage. No one has the right to invade another's physical privacy. Physical privacy rights are not given to anyone at birth. Every single person has a wonderful sense of wellbeing. People mostly desire to protect their "private rights" for this reason. The individual's right to privacy fosters an atmosphere conducive to the pursuit of knowledge concerning the person's non secular life. Because it protects one's right to free expression, affiliation, and personal choice, privacy is, once again, one of the cornerstones upon which our democratic society rests. Without personal space, it's humanly impossible to function well. Recent innovations made possible by the idea of personal privacy have dramatically improved people's standard of living. There are now unparalleled methods of human monitoring in use by every public and private enterprise in the global economy. No longer to a large extent, pervasive surveillance drives a person to behave towards his typical behaviour. Because of this, an individual is unable to think or judge by themselves, form selected relationships or businesses, speak carelessly, act independently, etc. This paper will explore the misuse of media tools in the modern era, when more and more media tools are being developed and humans don't know the limitations to utilise them. The Researcher will investigate how the expansion of technology into increasingly private areas might influence people's everyday lives

¹ Ph.D Research Scholar, Department of Law, Pandit Deendayal Upadhyaya Shekhwati University, Sikar, Rajasthan-332024

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

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

and freedoms. We'll also talk about how far—and in what new ways—an individual's privacy needs to be guarded in the modern, digital world. In addition, the report will provide a summary of the ways in which the government has handled data privacy via legislation and regulatory frameworks.

KEY WORDS: Privacy, Right, Human and Physical.

Introduction

Nowadays, people rarely, if ever, wait in line for anything; after placing an online order, they receive their goods at their front door. Thanks to advancements in computing, this is now possible. Communication, access, sharing of information, and transparency are all improving because of the internet's expansion and development. Of course, there are always going to be drawbacks to something, as the old adage goes. As the internet becomes more widely used as a medium for the communication of personal, confidential, and business-related information, the corresponding growth in its misuse is also inevitable. Being autonomous entities, humans are said to naturally desire privacy and control over some areas of their existence. Human behaviour has an innate desire for privacy that is unalienable and is today acknowledged as a basic human right. As each person's privacy is fundamental to their life and liberty, it must be preserved. The need for this right to privacy has occasionally been acknowledged by academics and judges, and it currently occupies an unassailable position in contemporary life.

Even in India, the right to privacy is not explicitly stated in the country's Constitution, but it has been included in the category of fundamental rights according to court interpretation. Man has become more sensitive to publicity as a result of the intensity and complexity of the developing society, making solitude and privacy more important for an individual. Nonetheless, since society has developed, contemporary businesses have uncovered a number of items that result in privacy infringement. The age of information technology is currently upon us. A new world with improved communication, quicker information exchange, and greater transparency has emerged as a result of the development of the internet and the expansion of its accessibility. But each thing has advantages and disadvantages. Since the internet is being used more and more for the

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

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

interchange of sensitive, private, and business information, there is also an increase in technological misuse, which is generally unavoidable.

There is no new right to privacy. It was a common law principle that everyone who has their privacy violated has the right to sue for damages under the tort law. "Semayne's Case (1604)" was one of the earliest cases dealing with the aforementioned subject. The incident involved the London Sheriff entering a residence to carry out a legitimate writ. Although recognising a man's right to privacy, Sir Edward Coke stated that "everyone's house is to him as his castle and fortress, as well as for his defence against damage and violence, as well as for his relaxation." The idea of privacy continued to evolve in England in the 19th century and is now widely accepted worldwide. In *Campbell v. MGN*, the court found that "There is an intrusion in a circumstance where a person can fairly expect his privacy to be respected, and such intrusion will be capable of giving rise to liability unless the intrusion can be justified."

We live in the era of information, when any information is accessible with a few clicks. The proliferation of information has many benefits but also some drawbacks. By the use of various electronic devices and applications, there has been a significant growth in the volume of data generated during the past ten years. Data is generated and is all around us in almost everything we do.

Indian Jurisprudence on Right to Privacy

Article 21 of the Indian Constitution says, "No person shall be deprived of his life or personal freedom except in accordance with legal procedures." On August 24, 2017, the Supreme Court said that Part III of the Indian Constitution protects the right to privacy as a fundamental right. This decision about the laws and rules will have a big impact on a lot of people. Article 21 of the Indian Constitution says that new rules will be judged by the same standards that are used to judge laws that violate personal freedom. The right to privacy is now clear. The question that still needs to be answered is where its edges and limits are.

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

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

India doesn't have any comprehensive data protection or privacy laws. In essence, the rules and regulations in place today are sectoral. The Information Technology Act, 2000 and its rules, in addition to other sectoral laws, currently regulate how "private information" and "sensitive private data or information" are collected, processed, and used by corporate bodies in India.

In the case of *M. P. Sharma and Ors. v. Satish Chandra*(AIR 2008 SC 582), District Magistrate, Delhi and Ors., where the warrant granted for search and seizure was questioned in accordance with Sections 94 and 96(1) of the Criminal Code of Procedure, the Supreme Court first considered whether the "right to privacy" is a fundamental right. The search and seizure power was upheld by the Supreme Court as not violating any constitutional clauses. The Court also declined to acknowledge the right to privacy as a fundamental freedom protected by the Indian Constitution.

After that, in the case of *Kharak Singh v. State of Uttar Pradesh and Ors.*(AIR 1963 SC 1295), the Court considered whether it would be an abuse of the right guaranteed under Article 21 of the Indian Constitution to watch over an accused person's nighttime home visits, raising the question of whether Article 21 included the right to privacy. The Supreme Court decided that such monitoring did, in fact, violate Article 21. As a result, the right to privacy could not be understood as a basic right, according to the majority judges, who also claimed that Article 21 did not clearly provide for a provision of privacy.

Hence, in *Gobind v. State of M.P.*(1975 AIR 1378), it was argued that the police's right to housekeeping violated the right to privacy guaranteed by Article 21 of the Indian Constitution. The Indian Supreme Court upheld the right to privacy as a fundamental right protected by the Indian Constitution, and it ruled that police laws violated the principle of private liberty. However, the court encouraged the right to privacy to be developed on a case-by-case basis and rejected the idea that it is an absolute right.

Current Technology and Data Protection

In the case of *K. S. Puttaswamy (Retd.) v. Union of India*(2017) 10 SCC, this issue was once more brought before the Supreme Court on the grounds that the Aadhaar Card Scheme violated

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

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

citizens' fundamental rights to privacy, which are enshrined in Article 21 of the Indian Constitution, by collecting and compiling population and biometric data for various purposes. The Court submitted the case to a constitutional panel made up of nine (9) justices because of the uncertainty surrounding the constitutional standing of the right to privacy based on earlier legal rulings.

Unfortunately, India has not yet passed any explicit data protection legislation. The Information Technology Act of 2000 and the Information Technology (Reasonable Security Policies and Processes and Sensitive Personal Information) Rules of 2011 are the main laws that address data protection (also known as IT Rules). Regarding the gathering and disclosure of sensitive personal data or information, the IT Regulations set new responsibilities on commercial and business entities in India.

It contained a number of new regulations that mandated that businesses and organisations that process personal data seek the written authorization of the data owner prior to engaging in specific activities. The Information Technology (Amendment) Act of 2008 adds sections 43A and 72A to the IT Act of 2000, which had undergone some amendments before to its introduction. A person who suffers a wrongful loss or wrongful gain is entitled to compensation under Section 43A, which deals with the execution of acceptable security standards for sensitive Personal data or information.

The provision includes passwords, financial information (such as bank account or credit card details), physical, physiological and mental health status, sexual orientation, medical records and history, and biometric information as sensitive personal data or information. A violation of Section 72A is punishable by imprisonment for up to three years and/or a fine of up to Rs. 5,000,000 for a person who causes wrongful loss or wrongful gain by disclosing the personal information of another person while providing services pursuant to a valid contract.

Under rule 5 of the IT Regulations, 2011, a body corporate or person acting on its behalf may not collect personal data or information unless it is gathered for a legitimate purpose relating to a functional activity of the body corporate and the collection of such information is required for that purpose. In addition, the person whose information is shared must be informed of the

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

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

collection of the information, its purpose, the intended recipients, the name and other details of the agency collecting the information, and the agency holding the information.

Each entity or anyone in possession of data subjects' personal information is prohibited from keeping it for longer than is necessary and from using it in ways inconsistent with the purposes for which it was gathered. The data subject is free to agree to the collecting of his data or to decline, and he is also free to revoke his consent at any moment. Even for the aim of exchanging information with third parties, permission is essential.

However, in cases where the information is being shared with government agencies that are required by law to obtain information (including sensitive personal data or information) for purposes of identity verification, or for the purpose of preventing, detecting, investigating (including cyber incident investigations), prosecuting, and punishing criminal acts, no such consent from the information provider is required.

The Personal protection Data Bill, 2019

A Committee of Experts led by Justice B. N. Srikrishna was established in July 2017 to look into several concerns regarding data protection in India. The Committee provided the Ministry of Electronics and Information Technology with its report and a draught of the Personal Data Protection Law, 2018, in July 2018. On December 11, 2019, the Minister of Electronics and Information Technology introduced the Personal Data Protection Bill, 2019 in Lok Sabha.

This Bill aims to protect people's privacy in relation to their personal data and to create an Indian Data Protection Authority to handle matters pertaining to people's personal data for the aforementioned purposes. The proposed law would apply to any processing of personal data that has taken place on Indian soil, including data that has been acquired, revealed, transferred, or processed in any other way.

- a) The Government of India, any Indian Corporation, any Indian citizen, or any person or body of persons incorporated in India; and

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

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

- b) Organizations based outside of India that deal with Indian residents' private information. After being introduced in Lok Sabha, the bill has been submitted to a Joint Parliamentary Committee, which is now preparing a report for the upcoming monsoon session.

An issue of privacy between Whatsapp and Facebook: a number of companies operating in India offer services to help people communicate with one another in secret, including Whatsapp and Facebook. Whatsapp is one example of a popular smartphone app in India. When Facebook, the world's largest social networking site, bought Whatsapp in 2014, the company promised users that their privacy would not be compromised. Whatsapp first appeared in 2010.

In 2016, Whatsapp announced improvements to its privacy policy, one of which is the sharing of its users' account information with Facebook. After the judgement of the Delhi High Court enabled the information provided over Whatsapp to be accessible under its new privacy policy, a plea was filed with the Supreme Court arguing that the policy modification violated the right to privacy of the users.

Nonetheless, the Court ordered Whatsapp to erase the data of users who deactivate the app and those who prefer to have the programme installed on their mobile devices until September 25, 2016. When Whatsapp introduced a new privacy policy in January 2021, it sparked a firestorm of controversy. Users of Whatsapp would be unable to choose not to have their information shared with Facebook under the new policy.

A petition challenging the new privacy policy was filed in the case *Karmanya Sareen v. Union of India* in February 2021. The petition argued that the privacy protection standards followed in India are much lower than those observed in European countries, amounting to discrimination against its Indian users. Notice and a request for responses have been issued by the Supreme Court.

Whatsapp has pushed back the deadline to update until May 15, 2021, in response to significant backlash. The Chief Justice of India, SA Bobde, along with Justices AS Bopanna and V Ramasubramanian, have formed a three-judge bench to consider the case.

Conclusion

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

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

One of one's basic rights is the right to privacy. It is a privilege that safeguards each person's inner existence from intrusion by both State and non-State actors and gives them the freedom to live their lives as they see fit. It is accurately stated that technology now makes it possible for both State actors and non-State actors to enter a citizen's home without knocking on the door. Who enters one's home, how one lives, and with whom one is in a relationship are all personal decisions.

Family, marriage, procreation, and sexual orientation are all significant parts of dignity that must be protected in the privacy of the home. Even if the owner gives someone permission to enter the home, this does not give anyone access. The only safeguard is that the other person's rights should not be violated or hurt.

Both the physical form and technology fall under this. Privacy is one of the most crucial rights to be protected both against State and non-State actors and be recognised as a fundamental right in a time when there are numerous, diverse social and cultural standards, and more so in a country like ours that takes pride in its variety. To ensure that the privacy of its citizens is not invaded, the legislature should take the necessary action.

The idea that privacy is not an absolute right and is subject to some reasonable constraints is supported by the fact that only a small number of factors, such as national security, etc., outweigh the worth of an individual's right to private. When the Personal Data Protection Law is passed and put into effect, it is hoped that it will close the present gap between technology and the legal system. Advanced technology calls for more advanced legislation.

References:

1. The Constitution of India, 1949.
2. The Information Technology Act, 2000.
3. <https://www.legalserviceindia.com/legal/article-5404-right-to-privacy-in-digital-era-a-study-with-indian-context.html>
4. <https://blog.iplayers.in/data-privacy-in-digital-age-indian-perspective/>
5. [https://amity.edu/UserFiles/aibs/37f9Article-IX%20\(Page%2066-74\).pdf](https://amity.edu/UserFiles/aibs/37f9Article-IX%20(Page%2066-74).pdf)

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

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

6. Universal Declaration on Human Rights,
http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf
7. Courts judgement on Right to Privacy,
[http://supremecourtfindia.nic.in/pdf/LU/ALL%20WP\(C\)%20No.494%20of%202012%20Right%20to%20Privacy.pdf](http://supremecourtfindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf)
8. AnuragVaishnav, “The Personal Data Protection Bill, 2019: All you need to know”, The PRS Blog, December 23, 2019, available at <https://www.prsindia.org/theprsblog/personal-data-protection-bill-2019-all-you-need-know> (last accessed on feb 02, 2023)
9. Whatsapp Facebook Privacy, by Supreme Court Observer, available at <https://www.scobserver.in/court-case/whatsapp-facebook-privacy-case> (last accessed on feb 25, 2023)



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

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