



INDIAN JOURNAL OF
LEGAL REVIEW

VOLUME 4 AND ISSUE 1 OF 2024

INSTITUTE OF LEGAL EDUCATION



INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN – 2583-2344

(Free and Open Access Journal)

Journal's Home Page – <https://ijlr.iledu.in/>

Journal's Editorial Page – <https://ijlr.iledu.in/editorial-board/>

Volume 4 and Issue 1 of 2024 (Access Full Issue on – <https://ijlr.iledu.in/volume-4-and-issue-1-of-2024/>)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 – info@iledu.in / Chairman@iledu.in



© Institute of Legal Education

Copyright Disclaimer: All rights are reserve with Institute of Legal Education. No part of the material published on this website (Articles or Research Papers including those published in this journal) may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. For more details refer <https://ijlr.iledu.in/terms-and-condition/>

PRIVACY AND DATA PROTECTION IN INDIA: AN ANALYSIS

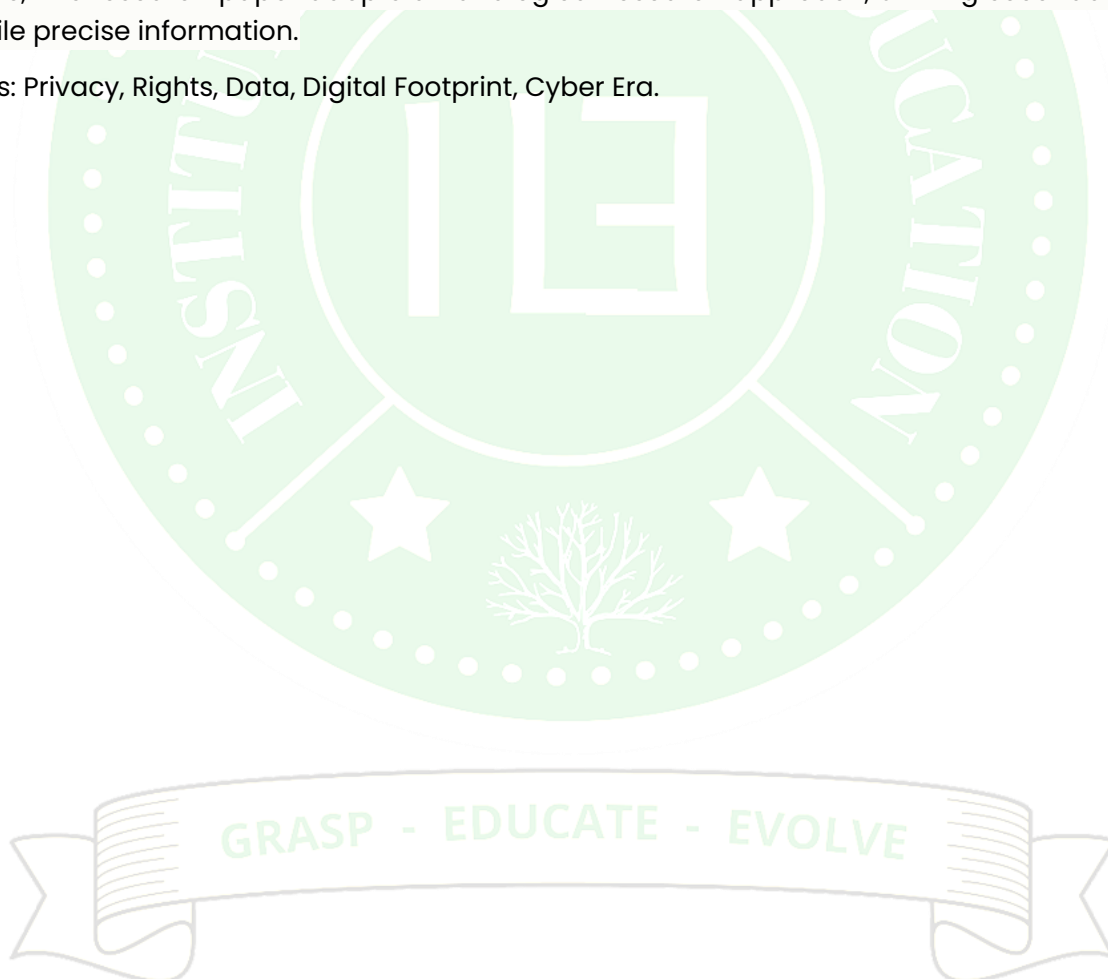
AUTHOR – PRIYANKA TOMAR, STUDENT AT ITM UNIVERSITY GWALIOR

BEST CITATION – PRIYANKA TOMAR, PRIVACY AND DATA PROTECTION IN INDIA: AN ANALYSIS, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 4 (1) OF 2024, PG. 1401-1406, APIS – 3920 – 0001 & ISSN – 2583-2344.

ABSTRACT

Privacy, deemed crucial for human survival, faces threats under the guise of legal procedures or public duties by officials. Imagine a world where individuals have no privacy rights, encompassing personal aspects like family, work, and relationships. Privacy, akin to oxygen for the body, ensures a peaceful life with dignity and liberty, as enshrined in Article 21 of the Indian Constitution. As society transitions into a digital era, characterized by increased social media and internet usage, data security²²⁴⁴ and protection become national imperatives. Data protection and privacy, intricately linked, form a critical and sensitive domain in contemporary legal discourse. Due to the COVID-19 pandemic, this research paper adopts an analogical research approach, utilizing secondary sources to compile precise information.

Keywords: Privacy, Rights, Data, Digital Footprint, Cyber Era.



²²⁴⁴ StartupFino: Authorship and Ownership of Copyright in India -

I. INTRODUCTION

The judiciary in India has recognized the Right to Privacy as an inherent right, similar to how developed countries like the USA, UK, and Russia have acknowledged it as a fundamental right for several decades. These countries understood the crucial role privacy plays in the sustainable development of a nation and in ensuring a peaceful life, which directly contributes to the prosperity of the country. In India, although the Constitution²²⁴⁵ and other legislations do not explicitly define or explain privacy, they have broad provisions that protect the individual privacy of Indian citizens. Landmark judgments such as the *Auto Shankar Case*³ and the *Puttaswamy Case*²²⁴⁷ have affirmed the Right to Privacy as a fundamental right according to the Hon'ble Supreme Court of India.

Furthermore, an important aspect closely related to the Right to Privacy is the concept of data protection. In today's digital age, where individuals spend more time on the internet, social media, and in the virtual space than in physical presence, the significance of data protection is equally crucial. Technology and law are interdependent, and it is expected that the future will witness a significant increase in reliance on Artificial Intelligence (AI) in the legal field. This will bring forth new challenges and obstacles concerning the Right to Privacy²²⁴⁸ and Data Protection in India and around the world.

We can observe how technology can infringe upon one's privacy and potentially cause disruptions in their life. Investigating agencies, for instance, have the ability to recover deleted chats, messages, and recordings from stored backups, referred to as the "Digital Footprint" of an individual on servers. While these actions may be legally justified when carried out by investigating authorities, in other

circumstances, except with the individual's consent, such acts can be seen as a direct violation of the Right to Privacy. In India, the Right to Privacy has been recognized as a fundamental right under Article 21 since 2017.

II. INTERNATIONAL SCENARIO FOR RIGHT TO PRIVACY AND DATA PROTECTION

The Right to Privacy and Data Protection is recognized as a fundamental and legally protected right in various parts of the world, in addition to India. These countries include:

1. United States of America (USA): In the USA, the Right to Privacy²²⁴⁹ is judicially recognized in both tort law and legislation. The Fourth Amendment of the US Constitution provides protection against unwarranted and arbitrary searches and seizures by state authorities. The US Supreme Court has recognized the general right to privacy under the Fourteenth Amendment, encompassing aspects such as family, marriage, motherhood, procreation, and child-rearing.
2. United Kingdom: In the United Kingdom, the Right to Privacy did not exist before 2000. However, after the enactment of the Human Rights Act in 2000, which incorporates the European Convention on Human Rights, the Right to Privacy became a legally recognized right in the UK. The act includes remedies for the violation of this right, covering aspects such as family, bodily liberty, and general privacy.
3. Russia: The Russian Constitution guarantees the right to privacy of personal life and family as a fundamental right under Article 23. Strict laws regulate the interception of communication and surveillance, requiring explicit consent unless performed by state authorities for valid reasons. Violations of privacy without consent can result in legal liability and criminal punishment under the Russian Federation's Code of Administrative Offences and Criminal Code.²²⁵⁰

²²⁴⁵ India Justice Foundation: *Balaji Motion Pictures Ltd. Vs. Bharat Sanchar Nigam Ltd*

²²⁴⁶ AIR 264

²²⁴⁷ AIR 2018 SC (SUPP) 1841,

²²⁴⁸ Right to Privacy verdict - en.wikipedia.org

²²⁴⁹ Understanding the Right to Privacy (R2P), civ gov

²²⁵⁰ Right to Privacy as a fundamental Right

4. South Africa: The Right to Privacy is constitutionally protected in South Africa under Section 14 of the Constitution. Individuals have the right to privacy, immunity from searches of their homes or property, and protection of their communications. South Africa has enacted laws such as the Protection of Personal Information Act and the

Regulation of Interception of Communications and Provision of Communication-Related Information Act to further safeguard privacy and data protection.

5. Japan: In Japan, the Constitution and the Civil Code provide for the protection of privacy rights. Article 13 of the Constitution safeguards personal information from arbitrary disclosure by public authorities. The Civil Code allows individuals to seek compensation under tort law for violations of their right to privacy.

Therefore, it is evident that the Right to Privacy and Data Protection is a global concern, not limited to India. Many developed and developing nations recognize the importance of privacy and data protection in today's era, where data is both a valuable asset and a potential vulnerability for individuals, corporations, and organisations²²⁵¹.

III. RIGHT TO PRIVACY AND DATA PROTECTION IN INDIA

The laws governing the Right to Privacy and Data Protection in India include:

1. Constitution of India: The Constitution of India guarantees certain fundamental rights to its citizens, including the right to privacy. Article 21,⁹ which protects the right to life and personal liberty, has been interpreted by the Supreme Court of India to include the right to privacy. This right to privacy encompasses the notion of data protection, and individuals can seek legal recourse in case of violations.

2. Indian Penal Code, 1860: The Indian Penal Code (IPC) is the primary criminal law in India. Several provisions of the IPC are relevant to the protection of privacy and data. For example:

a) Section 354-C: This provision deals with the offense of voyeurism, which involves capturing and publishing images of a person engaged in a private act without their consent. The punishment can range from one to seven years of imprisonment.

b) Section 354-D: This provision deals with the offense of stalking, which includes following a person without their consent or sending objectionable messages. The punishment can range from three to five years of imprisonment.

c) Section 379: This provision deals with the offense of theft, which includes unauthorized access to or copying of private data. The punishment can include imprisonment for up to three years or a fine or both.

d) Section 383: This provision deals with the offense of extortion, which includes putting someone in fear to deliver valuable documents or data. The punishment²²⁵² can include imprisonment for up to three years or a fine or both.

e) Section 471: This provision deals with the offense of using forged documents or electronic records. If such forgery infringes upon privacy or data protection, the punishment can include imprisonment for up to two years or a fine or both.

3. Information Technology Act, 2000: The Information Technology Act (IT Act) specifically addresses cybercrimes, frauds, and e-commerce. Its provisions are relevant to data protection and privacy, including:

a) Section 66: This provision deals with hacking, unauthorized access to computer resources or data, which can harm an individual's reputation or a corporate entity's goodwill. The punishment can include

²²⁵¹ International Journal of Creative Research Thoughts (IJCRT) ⁹ Right to Privacy (Article 21 of Indian Constitution), by testbook

²²⁵² DME Journals: Right to Privacy and Data Protection under Indian Legal Regime

imprisonment for up to three years or a fine or both.

b) Section 66C: This provision deals with fraudulently using someone's password to gain unauthorized access to their computer resources or data. The punishment can include imprisonment for up to three years or a fine.

c) Section 66E: This provision deals with the intentional capture, transmission, or publication of an individual's image without consent. The punishment can include imprisonment for up to three years or a fine.

d) Section 67: This provision deals with the publication or transmission of obscene material via electronic form. The punishment can range from imprisonment for up to three years to imprisonment for up to five years, depending on the conviction, along with a fine.

e) Section 67A: This provision deals with the publication or transmission of sexually explicit material via electronic form. The punishment can range from imprisonment for up to five years to imprisonment for up to seven years, depending on the conviction, along with a fine.

These are some of the laws in India that govern the right to privacy and data protection. It is important to note that there are other laws and regulations, such as the Personal Data Protection Bill, 2019 (not yet enacted as of my knowledge cutoff in September 2021), that further aim to protect personal data and privacy in India.

4. Copyright Act, 1957: The Copyright Act¹² protects the intellectual property rights of creators in India. While it was enacted during the pre-independence era, it remains a crucial law for protecting literary, dramatic, musical, and artistic works. The Act grants exclusive rights to the creators during their lifetime and extends for sixty years after their death. It prohibits unauthorized copying, replication, or use of the creator's work, especially for commercial purposes such as publishing, circulating, or transmitting the work. In case of infringement, the Act provides both civil and

criminal remedies. The victim can seek injunctions and damages in civil proceedings, while criminal penalties for infringement can include imprisonment of up to three years and a fine of up to two lakh rupees.

5. Indian Contract Act, 1872: Although not explicitly, the Indian Contract Act partially governs the right to privacy and data protection. This Act deals with the law of contracts, which are agreements between two or more parties for performing certain acts in exchange for consideration. Parties to a contract can include clauses relating to privacy or data protection, depending on the nature of the agreement. While the Act primarily focuses on contractual obligations and remedies, it indirectly contributes to protecting and safeguarding the right to privacy and data protection in India by allowing parties to define and enforce privacy-related terms in their contracts.

IV. JUDICIAL INTERPRETATIONS GOVERNING PRIVACY AND DATA PROTECTION IN INDIA

The Judiciary has consistently shown great attention and sensitivity when it comes to cases involving the infringement of an individual's fundamental rights as protected by Part III of the Indian Constitution. However, from 1954 to 2018, the Supreme Court of India has

¹¹ JSTOR: Privacy and Data Protection in India: A Critical Assessment . ¹² Student Manupatra: Copyright Act, 1957 (India)

presented differing opinions on whether the right to privacy is a fundamental right²²⁵³. It is important to recognize that privacy is an inherent and inalienable right of every human being, encompassing various aspects such as property, relationships, sexual orientation, and travel, where a reasonable expectation of privacy is warranted. While declaring the right to privacy as a fundamental right is beneficial for citizens, it also places additional obligations

²²⁵³ GeeksforGeeks: Copyright Act, 1957: Meaning, Features, Remedies and

on the state to protect the privacy of individuals within India's territory. Even in cases of infringement of privacy by private individuals, the government may be held accountable. Therefore, to gain a deeper understanding of the significance of the right to privacy and data protection, it is necessary to examine the judiciary's position on this matter in various key judgments. These judgments are outlined as follows:

1. In the first case, the District Magistrate issued warrants and conducted searches for disputed documents belonging to the Dalmia Group of Delhi based on a FIR under the Code of Criminal Procedure, 1973. The group challenged the validity of the search and seizure, arguing that it violated their right to privacy and fundamental rights under Article 19(1)(f) and Article 20(3) (self-incrimination). The case was referred to an eight-judge Constitutional Bench of the Supreme Court, which held that search and seizure conducted in accordance with established legal procedures, such as following the procedure established by law and obtaining an FIR and subsequent orders from the District Magistrate, is not invalid or unconstitutional. The Court also expressed the opinion that the Constitution does not recognize the right to privacy as a fundamental right in India.

2. The "Telephone Tapping Case"²²⁵⁴ involved a Public Interest Litigation (PIL) filed by a voluntary organization, challenging the tapping of politicians' telephones by the Central Bureau of Investigation (CBI) in the name of public security. The petitioners alleged that telephone tapping was a serious invasion of the right to privacy and a violation of Article 21 (right to life and personal liberty). The Supreme Court held that phone tapping constitutes a serious invasion of Article 21 and the right to privacy and should only be invoked in situations of public safety or grave danger to the public at large. The Court outlined guidelines for the exercise of Section 5(2) of the Indian Telegraph

Act, 1885, including the appointment of a review committee to regularly review phone tapping orders.

3. In the case challenging the Aadhaar Card Scheme initiated by the Central Government, which required citizens to provide their sensitive and private data, including biometric fingerprints, for various purposes such as booking cylinders, banking, and electoral voting, the Supreme Court's nine-judge Constitutional Bench overruled the decision in the MP Sharma Case²²⁵⁵ of 1954. The Court held that the right to privacy is a fundamental right protected by Article 21 of the Indian Constitution and cannot be infringed except through due process of law. The Aadhaar Card Scheme was deemed unconstitutional and violative of the right to privacy. A committee appointed by the Central Government is currently working on protecting sensitive data and citizens' privacy, as affected by the Aadhaar Card Scheme, and will submit a report on the matter.

In terms of remedies, since 2017, the right to privacy is considered a fundamental right in India under Article 21 of Part III of the Constitution. Therefore, if a citizen's right to privacy is infringed by the state, they can file a writ petition directly before the Supreme Court under Article 32. In cases that do not involve a violation of fundamental rights, individuals must follow the hierarchy of courts, starting with the appropriate High Court under Article 226 and Article 227, before approaching the Supreme Court.

V. EXCEPTIONS FOR RIGHT TO PRIVACY AND DATA PROTECTION

The Right to Privacy, as enshrined in Article 21 of our Constitution, is a fundamental right; however, it is not absolute and can be limited or suspended in exceptional circumstances. The Supreme Court of India has clarified that even during Emergency situations,²²⁵⁶ Article 21

²²⁵⁴ People'S Union For Civilliberties ... vs The Union Of India And Another on 18 December, 1996

²²⁵⁵ AIR 1954 SUPREME COURT 300,

²²⁵⁶ Vedantu: Right to Privacy - Key Elements and Restrictions

cannot be suspended. Despite being a fundamental right, there are exceptions to privacy, which are legally permissible and applicable. If privacy were an absolute right, there would be a risk of misuse, as observed in other countries, leading to a miscarriage of justice and undermining the purpose of the law.²²⁵⁷

Exceptions to the Right to Privacy include:

1. Procedure Established by Law: Article 21 states that the right to life can be restricted according to established legal procedures, indicating that the right is fundamental but

not absolute. This prevents potential misuse of the right and safeguards against miscarriages of justice.

2. Public Security: The interception of communication under Section 5(2) of the Indian Telegraph Act is permissible in situations of imminent risk to public safety. This action, if just and fair, does not violate the right to privacy, as it is crucial for immediate action to protect the public.

3. Public Duty: Public servants acting in their official capacity or performing sovereign functions are legally protected. However, if their actions are arbitrary, biased, or against the rule of law, they can face separate legal action for professional misconduct or moral wrongdoing.

4. Public Safety: Interception of communications under Section 5(2) of the Indian Telegraph Act is justified in cases where public safety or national sovereignty is at risk. In such critical circumstances, this action is not considered a breach of the right to privacy or data.

VI. SUGGESTIONS

Suggestions for enhancing the status of Right to Privacy and Data Protection in India include the following:

1. While India has various laws and constitutional provisions governing Right to Privacy and Data Protection, the absence of a specific enacted law dedicated to privacy weakens its enforcement and assurance compared to other countries.¹⁸

2. India lacks a dedicated Data Protection Authority, unlike other sectors that have specific statutory bodies like the Bar Council of India for lawyers and the Indian Medical Council for doctors. This absence of an executionary authority in the privacy field undermines the legal infrastructure and protection of rights in the country, contrary to guidelines set by the Supreme Court on citizen privacy protection.

3. The absence of an Adjudicating Officer or Compliance Officer for privacy¹⁹

infringements in India, unlike specialized officers in other fields like the Ombudsman for Banking Disputes or the Lokayukta for corruption complaints, forces victims to approach the Apex Court or High Court, burdening the judiciary and

¹⁸ Linklaters: Data Protected India Insights

¹⁹ StartupFino: Authorship and Ownership of Copyright in India, by data guidance

causing delays that hinder justice. Establishing a dedicated adjudicating officer would enhance the integrity and assurance of privacy rights in India.²²⁵⁸

4. Establishing fast-track courts in India to handle privacy infringement cases, child abuse, and crimes like sexual abuse of children facilitated through social media platforms would ensure swift resolution and stringent punishment for offenders, providing timely relief to victims and promoting justice.

VII. CONCLUSION

In our analysis, we have explored the significance of privacy for humanity's peaceful existence, akin to the critical role played by

²²⁵⁷ International Journal of Creative Research Thoughts (IJCRT): Right to Privacy and Data Protection Issues in India

²²⁵⁸ PRS India: The Digital Personal Data Protection Bill, 2023

Data Protection²²⁵⁹. Reflecting on ancient times, our forefathers emphasised the value of knowledge as the key to success and greatness, where the knowledgeable were revered as leaders. Today, this reverence has shifted to "Data," the most vital asset that can profoundly impact one's life and existence if mishandled. The misuse of data can lead to unimaginable harm, making it more crucial than material possessions like money or valuables, which can be regained if lost.

The importance of data and privacy pervades every aspect of human life, whether in business administration, where SWOT Analysis²²⁶⁰ relies heavily on opponent data, or in healthcare and legal sectors. Data plays a pivotal role in shaping outcomes favorably or unfavorably for individuals and organisations. Therefore, it is apt to consider Privacy and Data as pivotal factors determining success or failure for individuals, firms, corporations, and even nations. Hence, prioritizing the Right to Privacy and Data Protection is essential for any nation aspiring to thrive in the contemporary world.



²²⁵⁹ iPleaders: Data protection and data privacy laws in India -

²²⁶⁰ Khaitan & Co: Data Privacy & Protection Law in India, By khaitoon & Co.