Page 3335 - 3346 **DOI:** *https://doij.org/10.10000/IJLMH.117461*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 2

2024

Right to Privacy: A Critical Human Right in Digital Era

GURVINDER SINGH[1]

ABSTRACT

Right to privacy as enshrined in Article 12 of Universal Declaration of Human Rights is changing and widening its scope in modern digital era of internet. As much as digitalization is growing, the right to privacy is becoming more and more critical. India too is nowhere behind in recognizing this human right as fundamental one through its Constitutional Law specially allying it with Article 21 as right to life, several other civil and criminal laws and judicial trends. A specific set of cyber laws especially Information Technology Act of 2000 is also there. The unbridled usage of freedom of speech and expression, sharing private and confidential data bypassing regulations, media trials, unorganized internet news media, online character assassination and much more are biggest challenges faced by right to privacy now a days. In huge digital sea of information it becomes very difficult for implementing authorities to filter and tackle anti human rights narratives. It'll not be wrong to say that this very right is now on the stake when almost every hand has camera and internet connection. Where every hand is armed with abovementioned resources there is complete sense of negligence in minds that what is the importance of right to privacy and what are the laws and principles with which they are playing. The jurisdictional limitations, inadequate and obsolete training of staff and lack of proper resources are terrible issues for every state dealing with right to privacy violations. In this research article national and international human right laws related to right to privacy will be discussed and light will be thrown on the factors responsible due to which effective implementation is lacking. Beside this unethical networking and public mindset which are ignoring such an important right in digital world on socio-human level will also be discussed.

Keywords: *Privacy, Internet, Human Rights, Laws, Media*

I. INTRODUCTION

First of all it is necessary to understand definition of privacy under the shadow of legal developments and judicial mindset. Privacy is actually, "a sense of any person to exclude others from his certain things, feelings, information, physical exposure and expressing himself selectively." The term privacy also includes physical or biological presence of a being which

[1] Author is an Assistant Professor at Department of Law, Chaudhary Devi Lal University, Sirsa, Haryana, India.

 [ISSN 2581-5369]

he doesn't want to share with others. One thing to remember here is when someone is putting certain things into his privacy that means those things are special to him and he is 'sensitive' about those things.

II. IS RIGHT TO PRIVACY A HUMAN RIGHT?

Numerous countries incorporate the right to privacy in their laws and even constitutions, safeguarding citizens from unauthorized intrusions into their personal lives by governmental bodies, corporations or individuals. This protection ensures that individuals have the right not to be subjected to unwarranted invasions of their privacy.

Privacy stands as a fundamental right, crucial for preserving autonomy and upholding human dignity, forming the bedrock upon which numerous other human rights find their footing. It empowers us to erect barriers and establish boundaries that shield us from undesired intrusions into our lives, enabling us to determine our identity and dictate our interactions with the outside world[2]. By defining the scope of who can access our bodies, spaces, possessions, communications, and information. Privacy grants us the ability to govern and safeguard these aspects of our lives. It is a general phenomenon that fundamental rights take shape from human rights which differentiate us humans from other species.

International Treaties about Right to Privacy as Human Right

Over 130 countries have added privacy protection in their constitutional statements. These countries are completely or somehow driven by international treaties.

The right to privacy is enshrined in the Universal Declaration of Human Rights. Article 12 reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Even prior to the advent of the digital era and the worldwide apprehensions regarding technology-driven surveillance, the authors of the Declaration recognized the significance of safeguarding privacy. Breaches of privacy are categorized as either "interference" or "attacks," exerting adverse impacts on an individual's life and jeopardizing their other fundamental human rights.

The International Covenant on Civil and Political Rights (1966) says almost the same thing in Article 17:

[2] S. Choudhry , How To Do Comparative Constitutional Law in India: Naz Foundation, Same Sex Rights, and Dialogical Interpretation (2010), available at https://papers.ssrn.com/sol3/pa- pers.cfm?abstract_id=l 673378.

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

Other international documents talk about privacy rights, including

The United Nations Convention on Migrant Workers in Article 14;

The UN Convention on the Rights of the Child in Article 16;

The American Convention on Human Rights Article 11;

And the African Union Principles on Freedom of Expression in Article 4.

The Concept of Privacy

KJ Dearie, a product specialist and privacy consultant at Termly, explores three fundamental concepts prevalent in global privacy laws: transparency, accountability, and user control.[3]

1. **Transparency:** As a core concept in data privacy, gained prominence with the rise of social media over the past decade. It was the culmination of highly publicized incidents, such as the Facebook election scandal aka Cambridge Analytica - and the 2018 Google data breach, which brought the term "data privacy" into the mainstream lexicon with the significance it carries today. In response to the changing consumer attitude towards data collection, the law swiftly adapted, and in some instances, led the way, ushering in the era of transparency.

   One example of such legislative response is Australia's Privacy Act 1988, which was one of the early privacy laws and continues to evolve in tandem with technological advancements. A groundbreaking aspect of the Privacy Act 1988 is the requirement for companies to develop comprehensive privacy policies like the California Online Privacy Protection Act (CalOPPA).

What sets Australia's law apart from others is the depth of transparency it demands in privacy policies. For instance, the Privacy Act 1988 necessitates the disclosure of:

- The entities with which data may be shared.
- The methods users can employ to edit or request access to their data.
- The process to file privacy-related complaints or breach claims.
- The possibility of data transfer outside the country and the involved countries.

[3] https://www.legalserviceindia.com/legal/article-7836-privacy-right-to-privacy-law.html

These stringent disclosure guidelines have since been adopted by privacy laws worldwide, from the EU's General Data Protection Regulation (GDPR) to India's Personal Data Protection Bill 2018.

Today, due to established legal precedents and the growing concerns of the public regarding their personal data, it is inconceivable to encounter a privacy law without stringent transparency requirements.

2. **Accountability:** In 2018, data breaches exposed a staggering 446.5 million records in the United States alone. With data becoming an increasingly valuable asset and hackers continually finding ways around security systems, there is now a significant burden on companies to safeguard the data they gather, store, and share. One noteworthy development in this area is the California Consumer Privacy Act (CCPA), which extends its reach beyond California and grants Americans a groundbreaking consumer right - the ability to sue for privacy violations. According to the CCPA, if a California consumer's data is breached, they have the right to sue the company responsible for storing that data for any loss of privacy, even if there are no physical or monetary damages incurred. For businesses and websites worldwide, the responsibility of safeguarding individual privacy has often been a concept rather than a requirement. However, this law seeks to define responsible data collection and storage practices, as well as the potential consequences of negligence.
3. **User Control**: The new wave of privacy laws not only addresses company responsibilities but also empowers internet users with more control over their own data. Two major themes emerge from these new rights: firstly, users have rights over data already collected about them, and secondly, they have rights over the future collection of their data.

III. IMPORTANCE OF PRIVACY

This very right is important because it lays the foundation of so many others rights. Our fundamental right of speech and expression is deeply connected with right to privacy. Without protecting privacy it is impossible to protect freedom. When we talk about privacy it is generally about drawing boundaries to ensure protection but question is that who cares about our personal information and data[4]. The answer is very simple. Any individual in society can intrude into privacy of another just for his own mindset or to blackmail him, but it becomes very crucial

[4] A. Watson, Comparative Law and Legal Change, The Cambridge Law Journal 37(2) (1978), 313, 317.

 [ISSN 2581-5369]

when someone's privacy is violated by even more powerful entities like governments and corporations.

Government: In India a dispute was raised in 2021 when news was circulated through parliament session that government has purchased software named Pegasus which spyware from Israeli cyber-arms company NSO Group to spy on specific people. Similarly in 2013 according to a whistle blower from governmental agency NSA found spying on American residents. Governments have much more powerful sources and agencies by which it can spy on people as well as groups. There can be several reasons for doing so. 'National Security' is popular excuse given by governments for such privacy violations. But actually government can use such measures to alter opinion of people about their unjustified policies or to shut the mouth of whistle blowers which is quite adverse for general public as well as nation as whole. Private information of people can be used by governments as a tool to win elections unfairly.

Corporations: Meant for earning profit, the corporations can use private information of people for their own good. The data we feed or share with social media platforms or giving data usage consent to corporation websites including 'cookie consent' is very critical now a days. Your personal surfing on internet, searches you do online and your device input consent can be used to influence your opinion. That data can be used or sold by corporations to interested parties for showing you personalized ads or changing your opinion about certain things. In some cases it can go to complete mind wash of people by spreading hatred on the name of your religion, caste, creed, race etc.

IV. DATA RIGHTS AND PRIVACY PROTECTION

The EU's General Data Protection Regulation (GDPR) stands out as one of the most significant regulations safeguarding consumer data rights. Within its provisions, specifically in Articles 15-21, data subjects are granted various rights, including access, modification, deletion, and transfer of their personal data, which has been collected from them.

Similar to the GDPR, Brazil's Lei Geral de Proteção de Dados Pessoais (LGPD) also empowers data subjects with these fundamental rights. Additionally, LGPD introduces the right to an explanation, enabling data subjects to request information about the purpose and methods of data processing.

Modern data privacy laws not only enhance user rights over existing data but also introduce novel rights concerning the future collection and processing of data. A prominent example of this trend is the concept of cookie consent. Regulations like the ePrivacy Directive, commonly known as the EU Cookie Law, require websites to seek users' consent for data collection through

 [ISSN 2581-5369]

cookies. This consent is usually obtained through banners or modals that appear when visiting a website. Additionally, regulations such as ePrivacy mandate businesses to offer users the option to customize their cookie category preferences. For instance, a user can provide consent for a website to use analytics cookies while refusing the use of advertising cookies. An updated version of the ePrivacy Directive, known as the ePrivacy Regulation (institution date yet to be determined), is currently in development, promising more comprehensive guidelines regarding cookies.

The following excerpt is introductory chapter of the book titled "The Right to Privacy: A Doctrinal and Comparative Analysis," co-authored by Dr. Hilary Delany and published by Round Hall in 2008, conducts a conceptual examination of the right to privacy. This chapter serves as an essential overview of the main themes explored in subsequent sections of the book. It delves into the intricacies associated with defining the right to privacy, drawing on the works of various authors, including Judith Jarvis Thomson, Russell Brown, Warren and Brandeis, Ruth Gavison, Beate Rossler, Nicole Moreham, and Daniel Solove. The chapter presents an approach that substantiates the right to privacy as a fundamental element of a system that prioritizes and effectively safeguards human autonomy. Within this framework, privacy is understood to extend beyond the mere protection of secrets and confidentiality, encompassing the social dimension of human existence.. By safeguarding privacy, individuals are encouraged to actively participate in the social sphere, promoting experimentation, intimacy, and the development of personal and social identity.

Chapters exploring the notions of privacy: The following chapter delves into the distinctions between privacy as an autonomy value and privacy as a legally enforceable right. Attempting to define privacy solely as something related to individual or social identity proves impractical within legal contexts.[5]

Thus, the chapter proposes a three-fold categorization of privacy claims:

1. Decisional Privacy:

This pertains to an individual's entitlement to make their own decisions. Nonetheless, the chapter argues that considering this as independent legal right lacks coherence.

2. Spatial Privacy:

This involves a claim to privacy over a physical space, whether it concerns territorial privacy

[5]Cliodhna Murphy & Eoin Carolan & Hilary Delany et al, The Right to Privacy: A Doctrinal and Comparative Analysis (1t ed. 2008).

or the privacy of one's own body.

3. Informational Privacy:

This refers to a claim of privacy over specific information.

The chapter then proceeds to examine whether the right to privacy can be viewed as a means of exercising control over various dimensions. However, this control should not be seen as an absolute entitlement that completely bars access to the concerned area.

Privacy is a multifaceted concept, intricately tied to the context in which it operates. Therefore, the right to privacy empowers individuals to govern who may access a particular dimension and the permissible use of that access. The specifics of this right may vary depending on the unique circumstances of each claim.

Additionally, the chapter explores the correlation between privacy and freedom of expression. It argues that privacy and freedom of expression often complement each other, as safeguarding privacy can facilitate an individual's ability to freely express them.

However, conflicts between privacy and the media's freedom of expression may arise more frequently. It is crucial to acknowledge that individual expression rights and those of the media differ in nature and extent, necessitating a more nuanced understanding of how they relate to privacy.

V. LAWS IN INDIA

The Constitution of India does not explicitly provide for a standalone fundamental right to privacy. However, the judiciary has construed the right to privacy to fall within the ambit of other existing fundamental rights. Notably, the right to privacy has been interpreted in light of the freedom of speech and expression guaranteed under Article 19(1) (a) and the right to life and personal liberty enshrined in Article 21 of the Constitution of India[6]. Nevertheless, reasonable restrictions outlined in Article 19(2) upon these Fundamental Rights are subject to that the State may impose.

An outrageous development generated in the land mark leading case of Justice K S Puttaswamy (Retd.) & Anr. vs. Union of India and Ors[7]. In this instance, the constitution bench of the respected Supreme Court declared the Right to Privacy as a fundamental right, with the condition that it is subject to reasonable restrictions.[8]

[6]M.P. Jain, Indian Constitutional Law, (5th ed 2005), Wadhwa: Nagpur
[7] 26 September, 2018
[8] https://indiankanoon.org/doc/127517806/

 [ISSN 2581-5369]

Presently, India lacks specific legislation governing data protection or privacy. However, the relevant laws that address data protection in the country are the Information Technology Act[9], and the Indian Contract Act[10]. It is expected that a comprehensive law on data protection will be introduced in India in the near future as Data Protection Bill is pending in monsoon session 2023.

The Information Technology Act in India addresses compensation and punishment related to wrongful disclosure, misuse of personal data, and violation of contractual terms involving personal data can lead to significant consequences, both civil and criminal.

In accordance with Section 43A of the Information Technology Act, a body corporate that handles sensitive personal data negligently, resulting in harm or gain to any individual, may be held accountable for paying damages to the affected party. The compensation amount is not limited, making it crucial for organizations to ensure proper security measures are implemented and maintained.

To protect sensitive personal data or information, the Indian government introduced the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules in 2011. These Rules encompass various details, such as passwords, financial information, physical and mental health conditions, sexual orientation, medical records, and biometric data. Compliance with these Rules is mandatory for body corporates and individuals dealing with such sensitive information. In case of a data breach, the responsible party may be liable to pay damages to the affected individual.

Furthermore, under Section 72A of the Information Technology Act, 2000, intentional and unauthorized disclosure of information without the concerned person's consent and in violation of a lawful contract can lead to criminal punishment. The offender may face imprisonment for up to three years and a fine of up to Rs 5,00,000 (approximately US$ 8,000).

These regulations emphasize the significance of safeguarding personal data and the severe consequences for mishandling it, aiming to ensure better data protection practices in the digital age.

Please note that Section 69 of the Act contains a provision that deviates from the general rule of preserving privacy and keeping information confidential. It provides the Government with the authority to take action when certain situations arise, and it is deemed necessary to:

[9] Act 21 of 2000
[10] Act 9 of 1872

 [ISSN 2581-5369]

1. Safeguard the sovereignty or integrity of India,

2. Defending India,

3. Ensuring the security of the State,

4. Friendly relations in respect to other countries,

5. Sustaining of public order, or

6. Preventing incitement to the commission of any cognizable offense related to the above reasons,

7. Conducting investigations of offenses.

Under this section, the Government is granted the authority to issue orders to any agency of the appropriate Government to intercept, monitor, decrypt, or cause the interception, monitoring, or decryption of any information generated, transmitted, received, or stored in any computer resource. This includes information of a personal nature.

Additionally, if certain information is deemed to be in the public interest, the Government may request the disclosure of such information. This may pertain to activities that pose a threat to national security, violations of the law or statutory duty, or instances of fraud.

The Information Technology Act of 2000, commonly known as the "IT Act," serves to legally recognize electronic transactions, including electronic commerce, conducted through means like electronic data interchange. It facilitates the use of non-paper-based methods of communication and information storage for electronic filing with government agencies[11].

Section 415 of the Indian Penal Code (IPC) defines cheating as inducing a person through deception to deliver property, consent to property retention, or engage in actions they would not do if not deceived, resulting in harm or damage to that person's body, mind, reputation, or property. For instance, if person A shows a false sample of an item to person Z, leading Z to believe it matches the actual article and consequently persuading Z to purchase and pay for the false item, A would be considered cheating Z.

VI. CHALLENGES AND MEASURES TO PREVENT PRIVACY VIOLATIONS

The pace of technological advancement is swift, offering numerous opportunities to the advancement of the world through technology have undoubtedly brought numerous benefits; nevertheless, it has also posed significant risks to the protection of privacy rights. As mentioned earlier, surveillance is just one facet of this issue, with privacy violations extending to include

[11] N.S., Bindra, Interpretation of Statutes, (10th ed, M.N. Rao and Amita Dhanda).

 [ISSN 2581-5369]

data breaches, a lack of transparency surrounding the extent of such breaches, and data-holding companies evading responsibility. In 2020, the United Nations responded to these concerns by adopting a fresh resolution focusing on the right to privacy in the digital age. This resolution acknowledged that technological progress has empowered governments, businesses, and individuals to conduct surveillance, intercept communications, and collect vast amounts of data.

Moreover, the resolution recognized that while everyone's rights are impacted, women and girls are particularly vulnerable to these privacy threats. In such cases, violations of privacy intertwine with gender-based violence, sexual harassment, and discrimination. As society evolves, so should all human rights, including privacy rights, which must adapt at an even faster rate to keep pace with technology. No individual should be compelled to relinquish their privacy rights as a consequence of living in the digital age. So following are the challenges and measures to curb those challenges so that privacy can be protected at every cost-

1. First challenge is that people are not aware about their privacy rights and legal provisions so they get tortured easily without getting known of breach of their substantial human right of privacy. Others who are violating these rights are also unaware about their duty to respect privacy of others. This challenge can be measured through spreading awareness.
2. Secondly internet information system including social media platforms and websites should be taken care of by expert authorities so that unethical tools can be prevented from breaching privacy of people.
3. Thirdly lack of staff can be curbed by adequate recruitment of specialized staff and proper up to date training of them so that they can deal with upcoming challenges.
4. Governments and corporations should work and deal with private data of people ethically and responsibly. A proper justice delivery system providing exemplary punishment to wrong doers can help in checking privacy violations. End to end encryption techniques can be used by companies dealing with private data of people.
5. In developing countries mindset of people must change towards respecting privacy of others so that one can stop taking interest in personal matters of others.

VII. CONCLUSION

India does not have a dedicated data protection authority. However, the IT Act establishes the role of an adjudicating officer responsible for determining whether an individual has violated the IT Act or its regulations when the claim for injury or damages does not exceed 50 million

rupees. In cases where the claim surpasses this threshold, the matter falls under the jurisdiction of a civil court. The adjudicating officer appointed for each state government is the Secretary to the Ministry of Information Technology.

The adjudicating officer possesses all the powers vested in a civil court, including the ability to summon individuals, administer oaths for testimony, demand the submission of documents and electronic records, accept evidence through affidavits, and issue commissions to examine witnesses or documents.

Law enforcement authorities have the authority to investigate offenses under the IT Act, such as those specified in section 72 and section 72A.

For specific sectors like banking, telecommunications, and the medical field, the respective sectoral regulators hold jurisdiction and powers pertaining to data protection.

Regarding the legal obligations of the data protection authority, discussions on privacy matters date back to ancient times. From safeguarding one's body and dwelling to controlling personal information, the concept has evolved over time. In 1891, American lawyers Samuel Warren and Louis Brandeis famously described the right to privacy as the right to be left alone.

In a significant development in 1967, Alan Westin's work "Privacy and Freedom" defined privacy as the ability of individuals, groups, or institutions to determine for themselves the when, how, and to what extent their information is shared with others.

*****

 [ISSN 2581-5369]

VIII. REFERENCES

1. A. Watson, Comparative Law and Legal Change, The Cambridge Law Journal 37(2) (1978), 313, 317
2. Cliodhna Murphy & Eoin Carolan & Hilary Delany et al, The Right to Privacy: A Doctrinal and Comparative Analysis (1t ed. 2008)
3. M.P. Jain, Indian Constitutional Law, (5th ed 2005), Wadhwa: Nagpur
4. N.S., Bindra, Interpretation of Statutes, (10th ed, M.N. Rao and Amita Dhanda).
5. S. Choudhry , How To Do Comparative Constitutional Law in India: Naz Foundation, Same Sex Rights, and Dialogical Interpretation (2010), available at https://papers.ssrn.com/sol3/pa- pers.cfm?abstract_id=l 673378
6. Constitution of India 1950
7. Information Technology Act 2000
8. Indian Contract Act 1872
9. https://www.legalserviceindia.com/legal/article-7836-privacy-right-to-privacy-law.html
10. https://indiankanoon.org/doc/127517806/

*****