The Modern Need and the Right to Privacy in Cyberspace: An Analytical Study

***Anuprash Rajat**
Research Scholar, School of Law, IFTM University, Moradabad
****Dr. Upendra Grewal**
Research Supervisor, School of Law, IFTM University, Moradabad

Abstract

In today's fast-paced world, technology is the driving force behind human behavior and ways of operation in all aspect of work. Computers, information, and technology have replaced the traditional ways of doing things—manual intelligence giving way to artificial intelligence—because nothing is immune to technological innovation. Therefore, even if all of this has surely made people's lives easier, it has also brought out new difficulties with regard to security and the preservation of personal data that individuals submit, absorb, and amass when transacting online and utilizing internet services. In order to solve the privacy-related issue, a special law that satisfies international standards and is more frequently accepted than in most other wealthy countries must be proposed immediately. The "Personal Data Protection Act, 2023" was recently introduced and adopted by the Indian parliament to safeguard private information online. The digital personal data is the main emphasis of this Act. Section 2(h) of the Act provides definitions for data, along with several additional provisions pertaining to data protection. This article focuses on cyberspace privacy issues and advocates for greater implementation of the "Right to Privacy in Cyberspace." Although this right is not guaranteed by the Indian Constitution, it is reasonable to assume that it will be covered by legislation.

Keywords: *Cyber Law, Technology, Privacy, Right to Privacy, and Protection of Personal data.*

I. Introduction

The concept of an individual's right to privacy is multifaceted. It makes reference to an internet user's special ability to control the gathering, storing, and sharing of his personally identifiable information. A person's identification details, interests, and the personal information of people they are related to, together with information about their education, health, and finances, are all considered forms of private data. Private information may be cleverly used for a number of purposes, including government surveillance and profit-making for businesses. The Apex

Judicial Authority declared the "Right to Privacy" to be a basic right in August 2017, notwithstanding the Indian Constitution's lack of explicit recognition of this right.[1]

In India, there is currently practically any data protection legislation or data safeguarding body, despite a plethora of administrative measures. Nonetheless, India has made significant progress in acknowledging the right to privacy.

II. Right to Privacy in Indian Perspective

The Supreme Court ruled in *M.P. Sharma v. Satish Chandra*[2] that the Indian Constitution does not guarantee the right to privacy. The panel was debating whether Article 19(1)(f)[3] of the constitution of India is violated by a search warrant issued under Section 96(1) CrPC.[4]

The dissenting opinion of the Apex Court in *Kharak Singh v. State of Uttar Pradesh*[5] is particularly noteworthy as it acknowledged that Article 21 and 19(1)(d) of the Indian Constitution safeguard the right to privacy as a basic right. In the current instance, the Court was considering the rules for continuous monitoring included in the U.P. Police Regulations. Despite being charged with dacoity, the accused was ultimately found not guilty. As time went on, the Apex Court decided that situations involving families, the home, and other private matters were covered by the right to privacy and were subject to "compelling state interest."[6]

The Supreme Court ruled that the right to privacy was enlarged to include telecommunications during its discussion of the issue of telephone tapping and that doing so constituted a serious violation of one's rights. Furthermore, the Supreme Court acknowledged the distinction between mental and bodily privacy. The ruling in the case of *Unique Identification Authority of India v. Central Bureau of Investigation*[7] states that it is forbidden to provide biometric information on a person who has been given an Aadhar number to a third party without their express consent.

[1] K.S. Puttaswamy v. Union of India, AIR 2018 SC (SUPP) 1841.

[2] AIR 1954. SC 300

[3] Article 19(1)(f), The Constitution of India, 1950.

[4] Section 96(1), The Code of Criminal Procedure, 1973.

[5] AIR 1963 SC 1295

[6] Govind v. State of M.P., AIR 1994 826

[7] *Unique Identification Authority of India v. Central Bureau of Investigation*, 2014 SC

Subsequently, the landmark decision in *K.S. Puttaswamy v. Union of India*[8] was rendered, whereby the Unique Identity Scheme was evaluated concerning privacy concerns. The Indian Constitution Bench had to determine that the right to privacy is protected by the Constitution and, if therefore, where it originates, given that the document lacks a clear framework for privacy. This ruling clearly concluded that privacy is a basic right guaranteed by the Indian Constitution, setting it apart from previous cases.

In addition, the bench noted the broad range of data and how it is used by the government and businesses across the country, as well as the fundamental nature of privacy and a comparative study of privacy laws from different countries. Apart from the Telegraph Act, 1885, which regulated communication interception, Sections 43-A and 72-A of the Information Technology Act served as specific measures protecting an individual's personal data prior to the "Right to Privacy" being recognized as a fundamental right under Article 21 of the Indian Constitution. Companies that collected data are subject to requirements under the recently passed Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which aim to protect personal information.

III. Understanding the Cybercrimes

The Information Technology Act, 2000, is the only legislation in India which deals with cybercrimes, but does not define the term "cybercrime" clearly. Also, no other legislation in India defines such definition. However, any illegal behaviour that is carried out over the internet or with the assistance of computers is generally referred to as cybercrime.

To understand the cybercrimes, we can rely upon some general definitions which can be as follows:

- *Cybercrime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.*[9]

[8] Id. 1

[9] https://www.britannica.com/topic/cybercrime

- *Crime that is committed using the Internet, for example by stealing someone's personal or bank details or infecting their computer with a virus.*[10]
- *Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.*

Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.[11]

The following three definitions are provided by Professor S.T. Viswanathan in his work *The Indian Cyber Laws with Cyber Glossary*:

1. Any illegal activity where a computer is used as a tool or the aim of the crime, that is, any crime whose method or goal is to interfere with a computer's ability to function,

2. Any computer-related situation where a victim experienced or might have experienced loss and a perpetrator intentionally made or could have made a gain,

3. Any illegal, immoral, or inappropriate activity pertaining to the automatic processing and transfer of data is regarded as computer abuse.[12]

Therefore, it can be said that, technology development has brought forth new socioeconomic and political issues for society, and rather than assisting the government in managing these issues, it has led to the creation of complex new situations that are challenging to comprehend and even more challenging to address with the application of existing laws. The state apparatus lacks the resources and expertise necessary to combat contemporary crime.

Over the past three to four decades, computers have drastically changed modern civilization. It has not only made life easier, but it has also greatly aided in the social, economic, and cultural convergence of many parts of the world. Sitting in a room, one may now access any part of the world thanks to computer technology. The limitations of space and time have been eliminated

[10] https://www.oxfordlearnersdictionaries.com/definition/american_english/cybercrime

[11] https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

[12] Vishwanathan, S.T., The Indian Cyber Laws with Cyber Glossary, Ed 2001, P. 81

by modern technology. Though improbable given the amazing benefits of modern computers, this has led to a jurisdictional problem in the judicial system.

IV. The Concept of Right to Privacy

The term "RIGHT TO BE LET ALONE" was first used to define privacy in a landmark paper written in 1890 by Samuel Warren and Louis Brandeis, who would go on to become a Supreme Court justice. Since the 1940s, "privacy" has gained recognition as a fundamental civic liberty on a global scale. A section on privacy can be found in the 1948 Universal Declaration of Human Rights. Something like this is contained in the 1950 European Convention on the Protection of Human Rights and Fundamental Freedoms. *"The claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others"*[13] is a more contemporary meaning of "privacy."

V. Evolution of the Concept of Privacy

It is accurate to say that the idea of a "right to privacy" is not new. It is essentially taken from common law. A person may file a claim for invasion of privacy under tort law and seek damages for such an infringement. *Semayne's Case*[14] (1604) was among the earliest cases on this subject. The aforementioned case concerned the Sheriff of London's entry into a home to carry out a legitimate writ. The *"house of everyone is to him as his castle and fortress, as well as his defence against injury and violence, as well as for his repose"*[15], according to Sir Edward Coke, who discusses the individual's "Right to Privacy."

VI. Right to Privacy and International Measures

International initiatives have addressed and safeguarded the right to privacy as a component of human rights. The Universal Declaration of Human Rights was ratified by the UN General Assembly on December 10, 1948, and it has been a significant milestone in the history of human rights protection worldwide. The right to privacy is guaranteed by Article 12 of the Universal Declaration of Human Rights. It states that *"No one shall be the victim of arbitrary attacks upon his honor and reputation, or of arbitrary interference with his privacy, family, home, or correspondence."*[16] Everyone is entitled to legal defense against these kinds of

[13] Westin, Alan F. (Dr.), Privacy and Freedom, 1967.

[14] Semayne v. Gresham (1604) 5 Co Rep 91; ER 194 (Semayne's Case)

[15] Ibid.

[16] From Article 17 of the ICCPR, 1966

intrusions or assaults.

In response to a UN General Assembly resolution from December 2013, which addressed widespread concerns about government surveillance activities worldwide and their chilling effects on human rights, these principles were acknowledged in the report "the right to privacy in the digital age" published by the UN Office of the High Commissioner for Human Rights.[17]

As the digital era develops, a growing amount of corporate and public sector databases include personal data belonging to citizens and consumers. The issue of privacy is driven by three social concerns that are raised by access to such data in such databases. These concerns include people's worries about:

- Who is Responsible;
- How Private Information is shared or used; and
- How it is Safeguarded.

Numerous laws, rules, and standards have been established worldwide in response to these concerns. These include the privacy guidelines of the Organization for Economic Cooperation and Development (OECD), the Data Protection Directive (DPD) of the European Union (EU), the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada, the U.S. Gramm-Leach-Bliley Act (GLBA), and the Privacy Framework of the Asia-Pacific Economic Cooperation (APEC).

The widely recognized OECD, EU, and APEC Privacy Principles serve as the foundation for numerous privacy regulations across the globe. The US Department of Housing, Education, and Welfare (HEW) developed Fair Information Practices for the United States of America (US) in 1973. The Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data were established by the OECD later in 1980. In 1995, the EU Data Protection Directive was released, requiring Member States to enact legislation complying with the directive. Eight important guidelines for the security of personal data are outlined in the OECD Privacy Guidelines. Relatively speaking, the APEC Privacy Framework was approved in 2004 by the ministers and leaders of the organization.

While there are similarities throughout different privacy frameworks and norms, customer perceptions of privacy vary. While the United States addresses consumer privacy through

[17] “Submission to report on the Right to Privacy in the Digital Age by the Office of the UN High Commissioner for Human Rights”, https://www.accessnow.org/

sector-specific and state laws on privacy of data about consumers that are administered by a variety of agencies, the European Union addresses privacy of personal information through a single omnibus law and through a recognized and independent data protection authority. These include, among other things, legislation protecting financial and health information. A range of organizations and self-regulatory methods complement these regulations.

The Data Protection Directive (DPD), issued by the European Union, mandates that Member States adopt data protection. The Directive lays out possible exemptions, including model contracts and consent. Binding Corporate Rules (BCRs) have been added to the list of derogations. The US has a track record of self-regulation, most notably through its *safe-harbor* agreement with the EU. The International Safe Harbor Privacy Principles[18], also known as the Safe Harbour Privacy Principles, were formulated between 1998 and 2000 with the aim of averting unintentional disclosure or loss of personal information by private organizations that store customer data within the European Union or the United States.

There were 7 principles evolved during this Safe Harbor Privacy Principles programme.

1. Notice: People must be informed by an organization about the reasons it gathers personal data regarding them, how to get in touch with it with questions or concerns, the kinds of third parties it shares the data with, and the options and channels available to them for controlling its utilization and disclosure. When people first receive a request to divulge personal information to an organization, or as soon as it is practical, this notice must be given in a clear and conspicuous manner. It must also be given before an organization uses the information for a reason other than the one for which it was actually collected, or reveals it to a third party.

2. Choice: A company must give people the option to decide (opt out) of having their personal information utilized or shared with outside parties. To exercise this option, they must be given clear, noticeable, easily accessible, and reasonably priced mechanisms. Affirmative or explicit (opt-in) choice must be provided for highly sensitive data, such as trade union membership, opinions on politics, religious or philosophical views, health and medical information, information showing racial or ethnic origin, and information about the individual's sexual life.

3. Onwards Transfer: An organization is only permitted to give third parties access to personal information in accordance with the concepts of choice and notification. If an organization is interested in transferring data to a third party and has not given users the option because the

[18] https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles

third party's use aligns with the original purpose of the data collection or was disclosed in a notice, it can do so only after verifying that the third party abides by the safe harbor principles or by entering into a formal agreement requiring the third party to guarantee at least the same degree of privacy protection as stipulated by the applicable safe harbor principles.

4. Security: In order to ensure that personal information is reliable for its intended use, organizations that create, retain, utilize, or distribute it must take reasonable steps to guard against loss, misuse, and unauthorized disclosure, alteration, and destruction.

5. Data Integrity: An organization is permitted to process personal data pertinent to the objectives of which it has been collected in accordance with these principles. An organization shall take reasonable measures to guarantee all information is precise, complete, and current, to the extent required for those purposes.

6. Access: People must be able to access their personal information that is held by an organization [reasonably] and have the ability to update or modify any inaccurate information. The type and severity of the data gathered, its intended uses, the cost and difficulty of giving the person access to the data, and other factors all play a role in how reasonable access is granted.

7. Enforcement: Mechanisms for guaranteeing adherence to the safe harbor principles, redress for those to whom the data pertains and who are impacted by failure to comply with the principles, and repercussions for the organization in the event that the standards are broken are all necessary components of effective privacy protection.

These mechanisms should, at the very least, consist of the following:

a. easily accessible and reasonably priced independent recourse mechanisms that allow individuals' complaints and disputes to be looked into, resolved, and, if applicable, damages awarded;
b. follow-up procedures that confirm the veracity of the claims and attestations businesses render about their privacy practices and that privacy adheres to have been set up as presented; and
c. obligations for organizations that announce their adherence to these principles to remedy issues arising from noncompliance and implications for such organizations. Sanctions need to be strict enough to guarantee that organizations follow them.

VII. Right to Privacy: Indian Constitution and various Aspects

"A person's privacy fosters individuality and, consequently, freedom." Nonetheless, the "Right to Privacy" is regarded as the most valuable and all-encompassing human right. The definition of privacy is a 'state' in which a person's life or affairs are not disturbed or disrupted, even though legal rights and universal conceptions were linked to privacy as two independent topics that required different treatment. While everyone has a different definition of privacy, the fundamental premise from which privacy is derived has existed for generations. Furthermore, through their rulings, the relevant courts are still developing the idea with regard to the Right to Privacy.

It was previously known that the Indian Constitution does not recognize the *"Right to Privacy"* as a Fundamental Right. Furthermore, because there was no clause in Article 20(3) that was in line with the US Constitution's Fourth Amendment, the Supreme Court of India dismissed the claims that a "Right to Privacy" existed in the matter of *Re M. P. Sharma v. Satish Chandra*.[19]

The case of *Kharak Singh v. The State of Uttar Pradesh & others*[20] subsequently examines the scope of the Right of Privacy in relation to the existence of regulations permitting the surveillance of suspects. Living alone is regarded as a right that includes the right to privacy. In terms of surveillance, it has been decided that monitoring activities that are invasive and gravely infringe upon persons' privacy may infringe against their right to freedom of movement, that is protected by Art. 19 (1)(d) of the Indian Constitution and Art. 21. Even though the Supreme Court started to acknowledge some minority viewpoints, Indian constitutional doctrine did not yet include the right to privacy.

Judge Mathew acknowledged that the right to privacy is a freedom under Arts. 19 (1) (a), (d), and 21 in the case of *Govind v. State of Madhya Pradesh*[21], but he also noted that this right is not unqualified. "Primitive rights are those that are explicitly granted to citizens, and one of those fundamental rights is the right to privacy. The purpose and background of the person being watched, as well as the boundaries and goals of the monitoring system, all contribute to

[19] (1954) 1 S.C.R. 1077

[20] AIR 1963 SC 1295

[21] AIR 1975 SC 1378

the fact that visits by occupants are not necessarily an irrational invasion of privacy. The individual alone has the right to privacy, not the location.

The right to privacy is manifestly protected by Part III of the Constitution's Peninsular Areas of Fundamental Rights, as noted by American jurisprudence, which Justice Matthews considered in her decision. In a different case, *Smt. Maneka Gandhi v. Union of India & Anr*[22], the Supreme Court ruled that "Personal Liberty" under Article 21 guarantees protection under Art. 19 of the Indian Constitution and displays a variety of rights. The Triple Test is as follows for any law that infringes against personal liberty:

1. Procedure established by law is provided by it;
2. It must pass the test of one or more fundamental rights outlined in Article 19 of the Indian Constitution, which may be relevant in a particular circumstance; and
3. It must pass the test of Article 14. The legislation and processes that permit interference with an individual's right to privacy and personal liberty must be just, equitable, and reasonable; they cannot be capricious, irrational, or oppressive in any way.

VIII. Right to Privacy: Current Scenario

The Supreme Court ruled in the most recent case, *K.S. Puttaswamy (Retd.) and Ors. v. Union of India and Ors*[23]., that the right to freedom under Article 21 of the Indian Constitution and the Fundamental Rights under *M.P. Sharma and Ors. v. Satish Chandra and Ors.*[24] and *Kharak Singh v. State of U.P. and Ors*[25]. would certainly lose their vitality and determination if the comments made in those cases were taken literally and initially interpreted as law. The ratio holds true in cases involving both institutional reliability and judicial discipline: a court's decision is superior instead of institutional integrity, and the lower court should not examine judicial discipline. The matter ought to be looked into and placed within the court's purview.

The *Puttaswamy Case*[26] ruling overturned the rulings of *M. P. Sharma*[27] *and Kharak Singh*[28], which held that the Indian Constitution does not recognize the right to privacy as a fundamental

[22] AIR 1978 SC 597

[23] (2017) 10 SCC 1: AIR 2017 SC 4161

[24] *Supra* Note 3

[25] *Supra* Note 6

[26] *Supra* Note 2

[27] *Supra* Note 3

[28] *Supra* Note 6

right. Similar to the aforementioned case, where a nine-judge bench ruled that the "right to privacy" should be regarded as a fundamental right and treated as the right to life under Article21. In the *Puttaswamy* ruling, the Supreme Court acknowledged that the Government's right to access personal information for valid national security reasons constitutes a justifiable constraint on the right to privacy. The Apex Court did, however, also stress that these exclusions have to be specifically designed and satisfy the four requirements outlined in the ruling. Kaul J. and Chandrachud J. summed these requirement as follows:

- **Legality**: Denotes that there must be a law in existence
- **Legitimate Goal**:

In view of Chandrachud J. 'A justifiable governmental goal ought to be the goal of the legislation.'

In view of Kaul J.- 'A democratic society must need the proposed action to achieve a justifiable goal.'

- **Proportionality:**

In view of Chandrachud J.- 'The goals and the strategies used to accomplish them should make sense'

In view of Kaul J.- 'The level of intervention must be commensurate with its necessity.'

- **Procedural Guarantees:** According to Kaul J. 'To prevent the misuse of government intervention.'

If the four tests are not followed, it will be considered a breach of Article 21.

IX. Privacy in the Cyber Space

Cyberspace is the term for a virtual environment made by computers. Generally speaking, citizens—also known as *'netizens'*—have been using the internet more and more in recent years to isolate their identities from their social circles. People tend to assume that these individuals are private and that they wish to protect their privacy. In actuality, it seems like there is a significant risk of personal privacy violations in the internet.

Every human being has a fundamental desire for privacy, which is to set boundaries around oneself that prevent others from entering. Interference or intrusion into another person's private life is forbidden by the right to privacy. The Indian Supreme Court has unequivocally stated in its rulings that the right to privacy is a basic freedom protected by the Constitution of India under Article 21.

It's estimated that 5.3 billion people use the internet, or nearly every single person, to communicate, post images, and share sensitive data on social media sites. Cybercriminals utilize computers as weapons or tools to obtain personal information, which they can then misuse and use against people, endangering their privacy.

The corporate world has seen numerous malfunctions thus far, including instances where a business employs an outside party to its benefits in order to steal critical files and information from other businesses, beat competitions, and establish itself as a best-selling enterprise. These days, internet data theft is a serious worry, and most nations have passed legislation to protect citizens' privacy.

Major Crimes Related to Privacy in Cyberspace

Cybercrimes, however, affects the society at a large. But, in this paper it is going to be discussed about the cybercrimes and privacy. Most cybercrimes attacks to the individual at first instance.

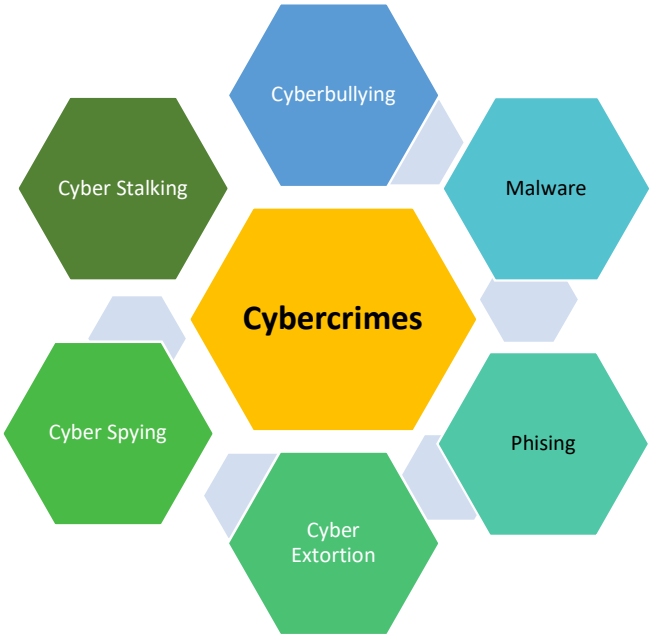

Fig1: Kinds of Cybercrimes

Cyberstalking: It is crime which is committed when someone uses the internet or any other method via online to stalk or harass another person online. It also includes online defamation, false accusation, or teasing. It is the straight example of breaching the privacy in cyberspace.

Phising: Phishing is a form of social engineering in which a perpetrator sends a bogus communication designed to trick or deceive a human victim. Typically, the goal of an attack is

to expose the victim's private information to malicious software that the attacker has written. It's a cyberattack that sends text messages, phone calls, or emails to certain people. Phishing can also take shape in the way of brand spoofing, in which users of the internet receive constant spam in their browsers after visiting an internet page that is a target.

Cyberbullying: Bullying through the use of the internet is known as cyberbullying. Social media, messaging apps, gaming platforms, and mobile devices can all be used for it. It is consistent behavior meant to frighten, enrage, or embarrass the people it is intended for.

Malware: Any software or computer program created with malicious intent is known as malware. Malware works to harm software or computer systems or steal data. Malware encompasses a range of online dangers, including ransomware, adware, spyware, and infections. Using malware for monetary gain is typically the aim of cyberattacks.

Cyber Extortion: Cyber extortion, sometimes referred to as cyber blackmail, is an unlawful act carried out by an individual who possesses important personal, professional, or business data. An individual engaging in this illicit digital activity is referred to as a "cyber extortionist."

Cyber Spying: The act of stealing secrets and information without the owner's consent or knowledge via methods on the Internet, networks, or personal devices by means of the use of proxy servers, cracking techniques, and malicious software such as Trojan horses and spyware is known as *cyberspying*, *cyberespionage*, or *cyber-collection.*

X. Right to Privacy and Right to Be Forgotten

In certain situations, the right to have one's personal information deleted from searches on the internet and other directories is known as the *right to be forgotten*. *"Determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past"*[29] is the driving force behind the issue. A person has the right to have information about them removed from the public domain, mainly through search engines, so that third parties cannot find it. There is no specific law in India addressing the right to privacy.

[29] Mantelero, Alessandro (2013). "The EU Proposal for a General Data Protection Regulation and the roots of the *right to be forgotten*". Computer Law & Security Review. 29 (3): 229–235

Nonetheless, Article 21 acknowledges the right to privacy, and the Indian judiciary is given the credit for this. Similarly, no article addresses the “right to be forgotten”, but the Indian judiciary is in charge of identifying and developing this concept.

The phrase "Right to be Forgotten" was first used in the 2014 case *Google Spain v. Maria Costa Gonzalez*[30]. In that case, Maria Costa claimed that his right to privacy had been violated when a Google search turned up an auction notice[31] for his repossessed home from 1998.

He claimed that Google and the media had violated his data. Upon referral to the Spanish Data Protection Authority, the newspaper was asked to remove Maria Costa’s personal data, but Google was requested to remove its users’ personal data because it processes user data on a regular basis and is not required to withdraw publishing.

The right to privacy was deemed a fundamental right by the Indian Supreme Court in 2017, yet it appears that this right is just stated in the Constitution, which some organizations have not actually observed. Similar to water, if data is not managed properly, it can overflow and have a profound impact on an individual's life. However, safeguarding the private information of its people is the government's first priority.

XI. Issues and Challenges: Right to Privacy and Cyberspace

In virtual spaces, the right to privacy has distinct meanings. Internet privacy refers to the right or obligation to maintain one's personal privacy with regard to the storing, using, disclosing to outside parties, and exhibiting of personal information online. Both individually identifiable information and non-personally identifying information, such as website usage or visitor behavior, might fall under the category of privacy. Any information which can be used to identify a specific person is referred to as personal identifying information.

1. Arbitrary and Unauthorized Interference: Legislators must make sure that a person’s right to privacy is not violated in an illogical or illegal way. At present, legal precedents prohibit government entities from violating an individual's right to privacy. A comprehensive legislation must offer defense against both private and public sector interference. In addition,

[30] C 131/12 (2014)
[31] https://blog.ipleaders.in/right-to-privacy-vis-a-vis-right-to-be-forgotten/

issues with audio and video monitoring, invasions of privacy, and communication interception (both electronic & digital communication) must be covered by the legal framework.

2. Medical Records: Medical professionals and medical insurers were the main users of medical records. However, the number of organizations and medical professionals with access to medical information has expanded with the development of internet-based records and massive databases of medical data. Although research that can enhance knowledge of illnesses and treatments for large populations is made possible by this availability, concerns have been expressed over possible abuse of this data due to the large number of parties who routinely have access to identifiable medical information. Without the patients' consent, it is imperative that no such data be gathered and sold to biomedical science researchers. The internet has made it more and more difficult to track this kind of data, which is not just a breach of privacy but also a violation of the confidentiality duty medical practitioners have to their patients. Nonetheless, if any action is done in the public interest, it cannot be deemed unconstitutional as defined by Article 47.

3. Banking and Financial Records: Since the number of fraud cases is rising quickly, it is also necessary to enact specific regulations to deter fraud and other crimes. Personal financial records must not be shared or shared among banks and other financial institutions without the owner's knowledge or consent, unless required by law. This is because doing so could lead to the abuse of such information, which would violate the right to privacy of the individual and possibly result in other crimes like extortion or kidnapping.

4. Cellular Phone Application Permissions: In order to offer self-help spot-on services, both public and private sector services have embraced the usage of mobile eservice models. For these services, a mobile device—such as an Android smartphone—must be used, and the smartphone's e-service app must be installed after the device user and the cellular device have submitted the necessary information. Users using mobile e-services have their security and privacy violated by data and information given through app permissions policies. Users of mobile app e-services are beginning to question the purpose of app permissions provided after installation for using of the e-service apps, as a result of the growing use of data analytics brought about by the availability of excessive amounts of data and information from unwitting mobile Android devices. Without the users' knowledge, political organizations and corporations have been using the data for years for campaigns, business analytics, and other

purposes such as gaining a competitive edge over rival companies. Users of mobile app e-services are now unknowingly exposed to security and privacy risks as a result.

5. Breach of Employees' Privacy: Most employers use the sensitive data by various methods. Employers usually keep biometric devices and sometimes use excessive surveillances of employees. Also, in various matters, CCTV are used for no use that is also a very common way of breaching the privacy.

XII. Suggestions and Conclusion

Suggestions

- **Adoption as Fundamental Right-** Right to privacy, however, not enshrined under the Indian Constitution as a fundamental right. It is only considered by the judicial notions. It is hope that ***'Right to Privacy'*** must be included as provision with reasonable restriction under the Indian Constitution.
- **Amend the Information Technology Act**: For the purpose of individual's protection and privacy in cyberspace, the IT Act, 2000 must be amended. There must be not only the penal provision under the Act, but also some provision regarding the cyberspace and privacy defined.
- **Awareness to Netizens:** There must be some awareness programmes or policies to aware netizens about cyber security, so that they can ask for more methods to protect. More awareness will result to the novel practical suggestions.
- **Awareness to the Personal Data Protection Act, 2023:** This Bill was awaiting from a long time. In India, it is a thorough legislative framework which is framed to maintain data privacy protection. The committee that addressed data protection in India and was chaired by *Justice B.N. Srikrishna* recommended the 'Personal Data Protection Bill, 2019'. The current Act aims to safeguard people's private information. But, very few people are aware about this legislation and it is need to be promoted, so that they can keep their data under privacy and untouched.
- **Reformation in Mobile Applications:** This is very common and seems mandatory in every chance, while using a mobile application, that the user is bound to give access and permissions like- gallery (storage), call logs, message, and other information in the device. So, it is needed that mobile applications must not ask for so much permissions and access

or there may be some options upon the user regarding permissions of the mobile applications.

Conclusion

One of the basic human rights is privacy. The Indian Constitution's Article 21 guarantees citizens' right to privacy as a necessary component of life and individual freedom. The right to privacy is shielded against both arbitrary legislative and executive actions as well as from other threats. However, the right could only be interfered with by the State if it is backed by a legislation that is in effect. Since the development of digitalization has made the realm of privacy more vulnerable in both the real and virtual worlds, rules and safety precautions are ostensibly needed to keep up with this expansion. We have constitutional protections against invasions of privacy in addition to laws such as the Information Technology Act of 2000 and the Indian Penal Code of 1860 that address this issue. Nonetheless, India’s cyber law is still evolving, and it remains to be seen how it will eventually meet the demands of the people and society today.