International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Navigating the Digital Frontier: Safeguarding the Right to Privacy in Cyberspace

**Arpana Sharma**

Student of LL.M (CYBER LAW), IILM University

**ABSTRACT**

The rapid evolution of technology and the pervasive integration of digital platforms into our daily lives have raised crucial concerns regarding the right to privacy in cyberspace. This research paper explores the different dimensions of privacy in the digital realm, focusing on the challenges, legal frameworks, and ethical considerations associated with safeguarding the Fundamental Rights and Directive Principles of State Policy. From a historical perspective to contemporary issues, the paper navigates the evolution of privacy, assessing the impact of technological advancements and the emergence of digital platforms. It critically evaluates international and national legal frameworks, emphasizing the difficulties in enforcing privacy laws across borders. The discussion also encompasses threats to privacy, including data breaches, surveillance, and corporate data collection, along with technological innovations and ethical considerations in response to these challenges. Case studies highlight both the consequences of privacy breaches and successful implementations of protection measures. Looking forward, the paper identifies future trends, challenges, and recommends strategies for enhancing privacy protection. This comprehensive analysis aims to contribute to the ongoing discourse on balancing innovation with the imperative to safeguard the right to privacy in the digital age.

**Keywords:** Privacy, Cyberspace, Technology, Udhr, Fundamental Rights, Violation

## INTRODUCTION

In the rapidly evolving landscape of the digital era, the transformative power of technology has permeated every aspect of our lives. As we navigate the interconnected web of cyberspace, the right to privacy emerges as a critical concern. The explosive growth of hi-tech Computer Science technology and its capacity to gather, store and process copious amounts of personal information has caused grave security threats to vital national infrastructure[1]. This sensitive and seemingly intractable problem of virtually unrestricted internet freedom has compelled to rethink the privacy parameters in the cyberworld[2]. The digital frontier, characterized by innovations such as social media, IoT devices, and artificial intelligence, presents both unprecedented opportunities and challenges to individual privacy. In this digital era, there is a growing interface between technology and society wherein, on one hand, advanced technologies assist to solve and alleviate a variety of issues in many sectors and on the other hand there is a constant concern that humans would become quiescent and excessively dependent on

[1] Tamara Dinev and Paul Hart, Internet Privacy Concerns and Social Awareness as Determinants of Intention to Transact, 10 International Journal of Electronic Commerce, 7-29 (Winter, 2005/2006).
[2] Robert S . Peck, The Right to be Left Alone, 15 Human Rights, 26-51 (Fall 1987).Published by : American Bar Association Stable URL : http://www.jstor.org/stable/27879466, 15 26–31 (2017).

technology.[3] The entire globe is evolving into a digital environment in which the internet and information and communication technologies play critical roles in the transmission of information.[4] Modern technical advancements have evolved in such a manner that there is a comparatively low-priced means for easy access to a vast and ever expanding range of information on individuals residing worldwide. As more and more internet users browse the internet and post their personal information; in the form of date of birth, educational qualification, marital status, private selfies, videos, family photos, hobbies and interests, online on social media networking websites are easily accessible to the general public which led to the scam of loss of personal data such as the *KOOBFACE*, a malicious malware which is composed of various components, with specific functionalities. Most of the malware cram their functionalities into one file, but *KOOBFACE* divides each capability into different files that work together to form the *KOOBFACE* botnet.[5] And as a repercussion of their lack of knowledge and ignorance about how these sites function, an individual's privacy is violated. In the case of youth and teenagers who constitute majority of the internet users and are susceptible in understanding the risk of exposing themselves to the cyber world. The social networking sites which are now used extensively for social interactions between the individuals by uploading their personal content such as age, race, gender and sensitive information, has further aggravated the issue of '*internet privacy*'.

Private data can potentially be creatively exploited for a variety of objectives, such as commercial profit generating, government monitoring and identity theft which can undermine national security as well. Although Constitution of India did not expressly recognized "Right to Privacy" as a Fundamental Right, yet the Apex Judicial Authority decided it to be a Fundamental Right, in August 2017.[6] The right to privacy is one of the fundamental Human rights. The human beings by their very nature require a space exclusive from interference of any kind which is necessary for the development of their individual personality. The fact that the right to privacy finds a special mention in the ancient texts as well and sources signifies its importance to the societies of all times. This right has received recognition and protection in societies of all times. In modern period, the human rights movements have considerably affected the notion and jurisprudence of legal rights. The right to privacy has grounded in explicitly in all international instruments concerning human rights.[7] This right enjoys a status of basic human right, which the State parties to this Human Rights Instruments are under an obligation to protect. It is for this reason that the nations all over the world have rendered and incorporated provisions in their legal system to ensure protection to the Right to Privacy. And in India, the right to privacy has received the highest protection as fundamental right under the Constitution of India.

## WHAT AMOUNTS TO PRIVACY INFRINGEMENT IN CYBERSPACE?

All of this discussion portrays that there is a shift from the industrial to the technological era, which has

[3] A.Kumar and Das, Interface between Technology and Society: A Study of the Legal Issues (120-127) (University of North Bengal, 2017).
[4] Umang Joshi, Online Privacy and Data Protection in India: A Legal Perspective, (95-111) (7 NUALS LAW JOURNAL , 2013).
[5] A typical KOOBFACE infection starts with a spam sent through Facebook, Twitter, MySpace, or other social networking sites.https://www.trendmicro.de/cloudcontent/us/pdfs/securityintelligence/white-papers/wp_the-real face-of-koobface.pdf (Last visited Nov 15, 2023)
[6] K.S. Puttaswamy v. Union of India MANU/SC/0911/2017.
[7] Art.12 of the Universal Declaration of Human Rights and Art.14 and 17 of the International Covenant on Civil andPolitical Rights

resulted in the creation of a new domain called "Cyberspace". The word cyberspace does not have a single definition and is understood differently by different persons, nations, institutions, and authorities.[8] Cyberspace can be explained as "an artificial environment made up of interrelated and intertwined networks that make use of electronic and electromagnetic spectrum based ICT to generate, store, alter, share, and utilize information".[9] In simple words, a non-physical realm of information flow and communication between computer systems and networks is referred to as cyberspace.[10] The domain implies a "virtual space" although all information created is physically kept and can be copied and accessed. The cyberspace ecology runs on exchange of information. It is data which is of prime concern in cyberspace as there is a constant threat of information getting leaked or tampered with. In layman's terms, data is anything that represents information, knowledge, facts, concepts, or instructions.[11] Today, data is more than just information to be accessed in cyberspace; it is also a market worth millions of rupees.[12] With technological developments and their increasing utilization, there is a vast expanse of personal information transmitted across the internet. Social media, CCTV, drones, bio metrics, are just a few examples of technologies that have a substantial impact on personal data security.

By its very nature, cyberspace is not user friendly in terms of privacy. The content in the form of any information uploaded and shared by any individual on the internet is permanently saved in the form of link and is available for reference by anyone who is able to trace or hack it. The information of any kind may it bean email, the credit card details, the personal content like images and documents, the chats and messages in all formats etc. are all stored somewhere on the remote computer through which it may be accessed at anytime and by anyone unless few safety measures are strictly followed. Thus, it is in fact a contradictory to speak of absolute privacy protection over internet, as it is not possible at all. The stealing or hacking of any sort of information that one has shared on the internet leads to privacy infringement. This stolen information is misused by the hackers with the varying degree of gravity. The most common practice is 'spamming', in which the website preferences of the user are tracked and then unwarranted and unsolicited contents are distributed to the user based on his tracked website preferences. In addition, the internet users' share different kind of information while transacting on the internet, which may be in the form of texts and images concerning their personal and professional life such as the bank accounts details, credit card numbers, passwords, emails, chats and messages etc. The information thus shared is meant for a desired recipient and the user expects it to be used only by him to whom it is directed and only for the purpose for which it is shared. Of this information, the information shared on the social networking sites is more general in nature which can be accessed by considerably large population, while the information shared during the individual chat sessions or by email or on any commercial website for specific transaction is less general and is meant only for those with whom it is shared. In addition, the information shared either on social networking sites or any other website always has certain purpose and the user expects this information to be used only for the desired purpose and not

[8] Ashish Chibbar, Navigating The Indian Cyberspace Maze: Guide For Policymakers,(2020 ed., KW Publishers)
[9] Id. At 6.
[10] Ian Carnaghan, What exactly is cyberspace and cybersecurity?, IN CYBERSECURITY, https://www.carnaghan.com/what-exactly-is-cyberspace-and-cybersecurity/. (Last visited Nov 14, 2023)
[11] Section 2 (o) of Information Technology Act, 2000.
[12] F Cassim, Protecting Personal Information in the Era of Identity Theft: Just How Safe Is Our Personal Information from Identity Thieves. 18 POTCHEFSTROOM ELECTRONIC LAW JOURNAL 68-110 (2015).

otherwise. Any unauthorized access or use of this information results into serious inroads in the privacy of an individual.

In 1960s Internet was developed for better communication, resource sharing and research. With the advancement of 'e'- technology, everything becomes effortless to access as well as a pathway to commit crimes without any endeavour. Recent years have witnessed a series of "moral panics" regarding information accessible on the Internet and its use for criminal activities[13] such as cyber snooping, corporate espionage, cyber stalking, identity theft, vishing, website defacement, copyright infringement.

**OUTLINING THE INTERNATIONAL PROTECTION ON RIGHT TO PRIVACY**

Universal Declaration of Human Rights (UDHR) was the first milestone document which recognized privacy as international human right in 1948.[14] Other than the UDHR, numerous other international instruments also contain isolated privacy provisions. The international instruments that incorporate privacy provisions can be classified as:-
(1) the UN instruments and (2) the OECD instruments.[15]

Consequently, the international instruments with privacy provisions include, among others- (i) Universal Declaration of Human Rights, 1948 (UDHR); (ii) International Covenant on Civil and Political Rights, 1966 (ICCPR); (iii) Convention on the Rights of the Child, 1989 (CRC); (iv) International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990; (v) UN General Assembly Guidelines Concerning Computerized Personal Data Files, 1990; (vi) Reports of the UN Special Rapporteur on the Right to Privacy (2016-2020); (vii) UN Personal Data Protection and Privacy Principles, 2018; (viii) OECD Guidelines on the Protection of Privacy, 1980, and (ix) Revised OECD Privacy Framework, 2013.[16]

Through the UDHR, the 'right to privacy' became an international human right before it was constitutionally recognized as a fundamental right.[17] To recognize privacy as one of the human rights, Article 12 of the UDHR is stated as follows: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*[18] Eighteen years later since the adoption of the UDHR, privacy was recognized by ICCPR in Article 17 by using the similar language to Article 12 of the UDHR. The only difference between the two documents lies in the fact that Article 17 of the ICCPR added the word 'unlawful' two times; before the term 'interference' and 'attacks' in the texts of Article 12 of the UDHR. For instance Article 17 of the ICCPR, states that *"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or*

[13] Sean M. Zadig and Gurvirender Tejay, Emerging Cybercrime Trends: Legal, Ethical, and Practical Issues, http://www.irma-international.org/viewtitle/59936/> ( Last visited Nov 15, 2023)
[14] Universal Declaration of Human Rights, 10 December 1948, GA/Res/217A
[15] Information Technology Act 2000, India, *available at: https://www.nyulawglobal.org/globalex/Right_To_Privacy_International_Perspective.html#_edn46* (last visited Nov 14, 2023)
[16] Idib 14.
[17] Diggelmann O and Cleis MN, 'How the Right to Privacy Became a Human Right' (2014) 14 Human Rights Law Review 441.
[18] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III) (UDHR) art 12.

*correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*[19] The Convention on the Rights of the Child, 1989 (CRC) is another vital UN document that attempts to ensure, among others, a child's privacy interest which was adopted by the UN General Assembly (UNGA) Resolution number 44/25 of 20 November 1989, and it pledges for the protection of the diverse rights of the children, including the right to privacy. The privacy provisions of this convention are also comparable with Article 12 of the UDHR and Article 17 of the ICCPR. For instance, in Article 16 of the CRC, it is stated that *" No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. The child has the right to the protection of the law against such interference or attacks."*[20] The next UN initiative was the adoption of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 1990, which aims to protect various rights of the migrant workers and their family members, including privacy. Regarding the protection of privacy, this instrument contains the same wordings as the UDHR, ICCPR, and the CRC. Article 14 of the Convention, for instance, states that *"No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, correspondence or other communications, or unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks."*[21] Apart from protecting the right to privacy, the UN was found keenly careful about the protection of one's personal data as well which has been evident by the '*Guidelines for the Regulation of Computerized Personal Data Files*', was adopted by the UNGA through its Resolution number 45/95 of 14 December 1990. It is worth mentioning that the principles enshrined in the said Guidelines were mostly based on the key data protection principles outlined in the OECD Privacy Guidelines, 1980, and Convention 108 of the Council of Europe, 1981. However, the short titles of those principles are as follows -
(1) principle of lawfulness and fairness; (2) principle of accuracy; (3) principle of the purpose-specification; (4) principle of interested-person access; (5) principle of non-discrimination; (6) power to make exceptions; (7) principle of security; (8) supervision and sanctions; (9) transborder data flows, and (10) field of application.[22]

The UN efforts and promises for the protection of privacy have also been manifested apparently through the Reports of the UN Special Rapporteur on the Right to Privacy. Since 2016, the UN Special Rapporteur on the right to privacy has placed a total of 11 annual reports covering, inter alia, the state of privacy at the beginning of 2016; critical areas of work for the protection of privacy in the digital age, 2016; governmental surveillance activities from a national and international perspective, 2017; big data and open data interim report, 2017; security and surveillance, 2018; big data and open data, 2018; privacy, technology and other human rights from a gender perspective, 2019; the protection and use of health-related data, 2019; security and surveillance, health data, and business enterprises use of personal

[19] International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 17.
[20] UN General Assembly, Convention on the Rights of the Child (adopted 20 November 1989) United Nations, Treaty Series, vol. 1577, art 16.
[21] UN General Assembly, International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (adopted 18 December 1990) A/RES/45/158, art 14.
[22] UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990.

data, 2020; preliminary evaluation of the privacy dimensions of the coronavirus disease (COVID-19) pandemic, 2020, and artificial intelligence and privacy, and children's privacy, 2021.[23]

Historically the right to privacy has not been at the forefront of discussions within the international community and the United Nations. But this positions has changed since 2013 after the Edward Snowden revelations. The international community focused on addressing not only on the practices of state sponsored surveillance but also surveillance undertaken by modern communications companies.[24] Recent events such as 2013 Edward Snowden and 2018 Cambridge Analytical revelations have shown that there needs to be an international legal solution to communication surveillance by states sometimes referred to as the *Five Eyes7* states and by communication-based companies such as Meta. Activities which use surveillance without an individual's permission is in clear breach of Article 17 of the ICCPR. Despite the exposure of such practices (Snowden and Cambridge Analytical in particular) there has been a slow process of an agreement of how to bring these practices in line with international human rights law. However, till now no formal legislation has been enacted to protect privacy in India. Data Protection Bill is waiting in the pipeline.[25]

## EVOLUTION OF RIGHT TO PRIVACY IN INDIA

Be it the Mahabharata or Ramayana or Manu Smriti, they have all considered privacy to be an vital aspect of an individual's life. An analysis of these scriptures proves the existence of rules that would respect the privacy of an individual in ancient Indian society. In Arthashastra, Kautilya around 321-296 B.C. has prescribed a detailed procedure to ensure right to privacy while ministers were consulted. So, looking from the historical point of view, privacy can be considered to be civil liberty that is indispensable to the freedom and dignity of an individual. From the ancient history of India, as we gradually move further then we will observe that by the nineteenth and twentieth century, the so-called privacy was associated with that of inviolability of house of property.

Even though a discussion and debate did take place in the Constituent Assembly regarding the right to privacy. In December 1946, the Constituent Assembly constituted various committees whose main work was to provide reports to the Drafting Committee, which would in turn prepare a draft of the Constitution of India and it was at the Committee Stage that a Sub-Committee group did try to advocate the right to privacy to be a part of the Fundamental Rights.

From the beginning, there were strong differences of opinion related to the right to privacy, as members like A. K Ayyar, B.N Rau and M.K. Panikkar had a strong objection to right to privacy to be upraised to the status of Fundamental Right. In fact the most open criticism of right to privacy was done by Alladi Krishnaswami Ayyar and B. N. Rau, who were the members of the Constituent Assembly, the comments of both these members manifests their resentment towards the right to privacy.

[23] Ibib 14.
[24] United Nations Human Rights Council, Report by the Special Rapporteur on the promotion and protection of the right to freedom and protection of the right to freedom of opinion and expression, 2013, UN Doc., A/HRC/23/4
[25] Anjum Ansari," International Perspective of Right to Privacy", https://law.dypvp.edu.in/blogs/international-perspective-of-right-to-privacy (November 15, 2023)

Ayyar was of the opinion that granting the right to privacy and secrecy in correspondence would be disastrous, it would elevate every private/ civil communication to that of State papers which would adversely affect civil litigation where documents form an essential part of the evidence and on the other hand, B.N. Rau was primarily concerned with the interference of the right to privacy with investigative powers of the police authorities. Later Both Rau and Ayyar successfully persuaded the Advisory Committee to leave out provisions relating to the right to privacy.

Even during the ongoing sessions of the Constituent Assembly, there had been a couple of times when an endeavor was made to include right to privacy within the chapter of fundamental rights in Indian Constitution. For instance, like on 30th April 1947 Somnath Lahiri, one of the members of the Constituent Assembly had presented a proposal to make the right to privacy of correspondence the fundamental right, 'the privacy of correspondence shall be inviolable and may be infringed only in cases provided by law……..'.[26] However this proposal failed to get a positive response in the Assembly. After almost a year, on 3rd Dec 1948 another attempt was made by Kazi Syed Karimuddin to incorporate "The right of the people to be secure in their houses, papers, persons, and effects against unreasonable searches and seizures shall not be violated and no warrants shall issue but upon probable cause supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.''[27]

So, the Indian Constitution did not succeed to recognize the right to privacy as a part of the Fundamental Rights to be conferred to the citizens of India. But over a period of time the Supreme Court of India has played an important role to addressed a number of cases that has dealt with right to privacy in some form or the other and which has helped the right to privacy attain its rightful position as a part of Right to Life and Personal Liberty under Article 21.

In one of the earliest cases, the Supreme Court made a narrow interpretation by limiting itself only to the prescribed statutory regulation. It was **M.P. Sharma v. Satish Chandra**[28], where the Supreme Court on the issue of 'power of search and seizure' held that privacy cannot be brought under fundamental rights as it was something not related to the Indian Constitution.

A decade later there was another important case, **Kharak Singh v. The State of U.P.**[29] which dealt with the issue of surveillance and that whether the surveillance which was defined under the Regulation 236 of the U.P. Police Regulation led to the infringement of fundamental rights or not and that did right to privacy come under fundamental right or not. The verdict that was given by the Supreme Court denied that the right to privacy was a fundamental right and that it was not a guaranteed right under our Constitution and therefore the attempt to ascertain the movement of an individual merely in a way in which privacy is invaded is not an infringement of a fundamental right guaranteed under Part III of the Indian Constitution. And it however held that Article 21(right to life) was the repository of residuary personal rights and recognized the common law right to privacy. However in this case Justice Subba Rao did say that privacy is a facet of Liberty.

[26] Information Technology Act 2000, India, *available at "https://www.constitutionofindia.net/constitution_assembly_debates/volume/3/1947-04-30?paragraph_number=101#3.19.101*", (Last visited on Nov 15, 2023)

[27] Information Technology Act 2000, India, available at "*https://www.constitutionofindia.net/constitution_assembly_debates/volume/7/1948-12-03#7.66.11"* (Last visited on Nov 15, 2023)

[28] M.P. Sharma v. Satish Chandra, AIR 1954 SC 300

[29] Kharak Singh v. The State of U.P. , AIR 1963 SC 1295

The next case was **Govind v. State of M.P,**[30] even though this case was alike Kharak Singh case but the approach towards this case was very different. It upheld the validity of Madhya Pradesh Police Regulation Act of 1961, under reasonable restriction. The judicial approach was that there is an existence of right to privacy in terms of the different guarantees provided by Part III Fundamental Rights of the Indian Constitution. However, the Supreme Court also observed that in the absence of legislative enactment, the right to privacy will necessarily have to go through a 'case-by-case development' because just one single case will be inadequate to see the exceptions and consequences of right to privacy. But one cannot deny the fact that this case did broaden the scope of Article 21 so that the right to privacy could fall into it.

In the case of **ADM Jabalpur v. Shivakant Shukla**[31], the Supreme Court wanted to determine that whether the right to personal liberty is restricted by any restriction other than those which are contained in the Constitution and statute law and it establishes that the right to privacy may not be expressly guaranteed, but it may be implicit due to its inclusion in common law. Justice Khanna had observed: "Article 21 is not the sole repository of the right to personal liberty..…no one shall be deprived of his life and personal liberty without the authority of laws follows not merely from common law, it flows equally from statutory law like the penal law in force in India."

Then in **Maneka Gandhi v. Union of India**[32] case, the Supreme Court in a broader sense interpreted Article 21and stated that the term 'natural law' which included the right to personal liberty and rights of personal security were incorporated in Article 21 of the Indian Constitution.

**R. Rajagopal v. State of Tamil Nadu**[33] was one of the first cases which elaborated the development and the span of right to privacy in a comprehensive manner. The Supreme court had held that the right to privacy was implicit to the right to life and liberty which Article 21 guaranteed. It further recognized that a citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing and education amongst other matters. None can publish anything concerning the above matters without any consent and also that the right to privacy can be both an actionable claim and also a fundamental right.

In **Unique Identification Authority of India & Anr. v. Central Bureau of Investigation**[34] case which involved the Central Bureau of Investigation that had sought to access a huge database that had been compiled by the Unique Identity Authority of India for investigative purposes of criminal offence. However, in this case the Hon'ble Supreme Court stated that the UIDAI should not be transferring any biometrics information who has been allotted the Aadhar number without the written consent of the individual persons to any agency or third party. More so, the Hon'ble Court also stated that no person shall be deprived of any kind of services for want of Aadhar number in case he/she is otherwise eligible/entitled. The various authorities would have to modify their circulars/forms etc. so that compulsory requirement of Aadhar Number is not required in order to meet the requirement of the interim order passed by the Court forthwith.

In **JUSTICE K.S. PUTTUSWAMY (RETD.) & ANR. V. UNION OF INDIA & ORS**[35] case, the verdict was the outcome of a petition challenging the constitutional validity of the Indian biometric

[30] Govind v. State of M.P ; Supra note 4
[31] ADM Jabalpur v. Shivakant Shukla, AIR 1975 SC 1378
[32] Maneka Gandhi v. Union of India, AIR 1978 AIR 597, 1978 SCR(2) 621.
[33] R. Rajagopal v. State of Tamil Nadu, AIR 1995 SC 264.
[34] Unique Identification Authority of India & Anr. v. Central Bureau of Investigation., (Crl) No(s).2524/2014.
[35] JUSTICE K.S. PUTTUSWAMY (RETD.) & ANR. V. UNION OF INDIA & ORSAIR 2014 SC 2524.

identity scheme Aadhar. It was related to the Unique Identity Scheme that was discussed along with the right to privacy. The question that was placed before the court was whether a right like right to privacy was guaranteed under the Constitution or not. The Attorney General of India had however argued that privacy did not have a place in the fundamental right guaranteed to Indian citizens. Eventually, the Court decided that the question related to the right to privacy should be left to be discussed by a larger constitutional basis because all those judgments that denied the existence of the right to privacy were declared by the larger benches than the cases where the right to privacy was accepted as a fundamental right. Due to this an unresolved controversy emerged, that compelled the Court to refer this issue to a larger bench so that it could be settled.

The unanimous judgment by the Supreme Court of India (SCI) in Justice K.S. Puttuswamy (Retd) vs. Union of India is a resounding victory for privacy. The order signed by all nine judges declares: The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.

Finally, it was on 24th August 2017, that a historical judgement was made by the Supreme Court of India that stated the right to privacy to be a part of fundamental rights that was protected by the Indian Constitution. The Supreme Court declared that the right to privacy stems from the fundamental right to life and liberty and that it would be having a long lasting consequence. The Nine- Judge bench of the Supreme Court was involved in the case of Puttuswamy vs. Union of India that declared the right to privacy to be protected under Part III of the Constitution of India. The Judgment was in response to the reference made in connection with the challenge to India's National Identity project called Aadhar.[36]

**RIGHT TO PRIVACY IN CYBER WORLD**

Stealing someone's intellectual work or hacking into someone's private property is a complete violation of his right to privacy. Although the Indian constitution does not originally provide the "right to privacy" as one of the fundamental rights guaranteed to the Indian citizens but it is protected under Indian Penal Code (IPC).

Cyberspace can be described as a non-physical terrain created by computers. Most often than not, in the recent times, netizen have been increasingly making use of the cyberspace to isolate themselves from their social circle. It has been observed that these people are private and want to secure their privacy but in reality, it turns out that there is a serious threat of infringement of privacy of an individual in the cyberspace.

In order to recognize digital evidence and electronic records, the Information Technology Act came into force on 17.10.2000. The preamble of the above said act would read as follows:- "*An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto"*. This Act also recognized some forms of cyber crimes and provided punishments for the same. The cyber crimes made punishable under the Act are set out from sections 65 to 85 and the punishment prescribed thereunder, ranges from

[36] Sargam Thapa, "The Evolution Of Right To Life In India", Volume 10 Issue 2 Ser. I,(P 53-58)

imprisonment upto three years to imprisonment to life and any fine amount could be imposed. An upper ceiling limit ranging from Rs.1,00,000/- to Rs.5,00,000 is also prescribed. The cybercrime is an evolved state of traditional crimes and the common forms of the cybercrimes have been broadly categorized into two i.e. cyber crimes against person and cyber crimes against property.[37]

Right to privacy is an important natural need of every individual as it creates boundaries around an individual where the other person's entry is restricted. The Hon'ble Supreme Court of India has clearly affirmed in its judicial interpretation that Right to Privacy is an essential part of the Fundamental Right guaranteed under Article 21 of the Indian Constitution. So, whenever there is some cyber crime related to infringement of the person's private property or its personal stuff then the accused can be charged under violation of Article 21 of Indian Constitution, and prescribed remedy can be invoked against the accused.

Another relevant piece of statute in this regard is The Indian Telegraph Act, 1883. It governs the use of wired and wireless telephones, teletype, telegraphy, radio communications and digital data communications. And it gives the Government of India exclusive jurisdiction and privileges for establishing, maintaining, licensing, operating and oversight of all forms of wired and wireless communications within Indian territory. It also authorizes government law enforcement agencies to monitor communications and tap phone lines under conditions defined within the Indian Constitution. This act came into force on October 1, 1885. Since then, numerous amendments have been passed to update the act to respond to changes in technology.

The Telecom Commercial Communications Customer Preference Regulations 2010 is one of the regulations, which aims to prevent the service providers from arbitrary sharing of personal information. Thus, all the service providers are obligatory to take necessary measures to protect the privacy and information shared on their networks.

The Hon'ble Supreme Court has also dealt with the right to privacy in the context of interception of phone calls in the case of **Amar Singh v. Union of India**.[38] The question, whether interception of telephonic message /tapping of telephonic conversation constitutes a serious invasion of an individual's right to privacy was considered by Hon'ble Apex Court in detail in the case of **People's Union case**[39], wherein it was held as under:

*"We have, therefore, no hesitation in holding that right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed "except according to procedure established by law. The right to privacy — by itself — has not been identified under the Constitution. As a concept it may be too broad and moralistic to define it judicially. Whether right to privacy can be claimed or has been infringed in a given case would depend on the facts of the said case. But the right to hold a telephone conversation in the privacy of one's home or office without interference can certainly be claimed as "right to privacy".*

Telephone conversation is a part of modern man's life and often of an intimate and confidential character. Right to privacy would certainly include telephone conversation in the privacy of one's home

[37] Deepthi Arivunithi, "Cyber Space Vis-à-vis Right to Privacy", Available at *http://tnsja.tn.gov.in/article/Cyber%20space%20vis%20-%20corrected%20new%2012082018.pdf*, (Last visited on Nov 15, 2023).

[38] Amar Singh v. Union of India, 7 (2011) 7 SCC 69.

[39] People's Union for Civil Liberties (PUCL) v. Union of India, reported in (1997) 1 SCC 301

or office. Telephone-tapping would, thus, infarct Article 21 of the Constitution of India unless it is permitted under the procedure established by law."
Recently, Whatapp, widely used messaging app was also accused of infringing the Right to Privacy of individuals for which Whatsapp convinced its users that the messages sent by the users are encrypted and thus does not infringes the privacy of the people.

**THE INDIAN SCENARIO**

In the report '*Big democracy, big surveillance: India's surveillance state*' [40] published by *Open Democracy*, India's surveillance programs mostly started following the 2008 Mumbai terror attacks when it was proposed by the Ministry of Home Affairs first for creation of a **National Intelligence Grid** (NATGRID), which will give 11 intelligence and investigative agencies real-time access to 21 citizen data sources to track terror activities and these citizen data sources will be provided by various ministries and departments, otherwise called "provider agencies", and will include telephone records, bank account details, passport data and vehicle registration details, among other types of data.[41]

NATGRID is far from India's only data sharing scheme. The **Crime and Criminal Tracking Network & Systems** (CCTNS), which would facilitate the sharing of databases among 14,000 police stations across all 35 states and Union Territories of India, excluding 6,000 police offices which hold high position in the police hierarchy. An allocation of Rs. 2,000 crore (around USD 320 million) has been made for the CCTNS, which is being implemented by the National Crime Records Bureau under the national e-governance scheme. Apparently, sharing and linking databases are not enough for tracking criminals and terrorists. In September 2013 it was reported that the Indian government has been operating **Lawful Intercept & Monitoring** (LIM) systems, widely in secret. In particular, mobile operators in India have deployed their own LIM systems allowing for the so-called 'lawful interception' of calls by the government. And possibly to enable this, mobile operators are required to provide subscriber verification to the **Telecom Enforcement, Resource and Monitoring** (TERM) cells of the Department of Telecommunications. And in the case of the Indian government, the LIM system is deployed at the international gateways of large ISPs. The functioning of these systems is immune to interception by the ISPs and are under lock and key so as to be in the complete control of the government. Though the government has mandated checks for monitoring and protection of user privacy which is largely absent. In effect of it, all Internet traffic of any user is open to interception at the international gateway of the bigger ISP from whom the smaller ISPs buy bandwidth. Since the government controls the LIMs, it directly sends software commands and sucks out whatever information it needs from the Internet pipe without any intimation and information to anyone except to those within the government who send the Internet traffic monitoring commands. This monitoring facility is available to nine security agencies including the IB, the RAW and the MHA. The governments' monitoring system which is installed between the ISPs Internet Edge Router (PE) and the core network has an 'always live' link to the entire traffic which enables the LIM system to have access to 100% of all Internet activity with broad surveillance capability based not just on IP or e-mail addresses, URL's,

[40] MARIA XYNOU, Big democracy, big surveillance: India's surveillance state, https://www.opendemocracy.net/opensecurity/maria-xynou/big-democracy-big-surveillance-indias-surveillance. (last visited Nov 14, 2023).
[41] IT ACT 2000, Avaiable at https://www.opendemocracy.net/en/opensecurity/big-democracy-big-surveillance-indias-surveillance-state/ (last visited Nov 14, 2023).

HTTPs, FHTpc, tele-net or webmail but even through a broad and blind search across all traffic in the Internet pipe using 'keywords' and 'key phrases'[42].

In addition to LIM systems being installed, the Government of India runs the Central Monitoring System or CMS which is a clandestine mass electronic surveillance program installed by C-DoT, a government owned telecommunications technology development center and operated by Telecom Enforcement Resource and Monitoring (TERM) cells[43]. Rule 419B under Section 5(2) of the Indian Telegraph Act, 1885, allows for the disclosure of "message related information" Call Data Records (CDR) to Indian authorities. Call Data Records, otherwise known as Call Detail Records, contain metadata (data about data) that describe a telecommunication transaction, but not the content of that transaction. In other words, Call Data Records include data such as the phone numbers of the calling and called parties, the duration of the call, the time and date of the call, and other such information, while excluding the content of what was said during such calls. According to draft Rule 419B, directions for the disclosure of Call Data Records can only be issued on a national level through orders by the Secretary to the Government of India in the Ministry of Home Affairs, while on the state level, orders can only be issued by the Secretary to the State Government in charge of the Home Department. Other than this draft Rule and the 'amendment to clause 41.10 of the UAS License Agreement'[44], no law exists which mandates or regulates the Central Monitoring System (CMS). This mass surveillance system is merely regulated under Section 5(2) of the Indian Telegraph Act, 1885, which empowers the Indian Government to intercept communications on the occurrence of any "public emergency" or in the interest of "public safety", when it is deemed "necessary or expedient" to do so in the following instances:

- the interests of the sovereignty and integrity of India
- the security of the State
- friendly relations with foreign states
- public order
- for preventing incitement to the commission of an offense

However, Section 5(2) of the Indian Telegraph Act, 1885, appears to be rather broad and vague, and fails to explicitly regulate the details of how the **Central Monitoring System** (CMS) should function. As such, the CMS appears to be inadequately regulated, which raises many questions with regards to its potential misuse and subsequent violation of Indian's right to privacy and other human rights.[45]

This program also gives security agencies and Indian Income Tax authorities centralized access to the country's telecommunications network and the ability to listen in and record mobile, landline, satellite calls and **voice over Internet Protocol** (VoIP) and read private e mails, sms and mms and track the geographical location of individuals all in real time. It can also be used to monitor posts shared on social media such as Facebook, LinkedIn and Twitter and to track user's search histories on Google without

[42] Shalini Singh, Govt. violates privacy safeguards to secretly monitor Internet traffic, http://www.thehindu.com/news/national/govt-violates-privacy-safeguards-to-secretly-monitor-internettraffic/article5107682.ece (last visited Nov 14, 2023).

[43] IT ACT 2000, Avaiable athttps://en.wikipedia.org/wiki/Central_Monitoring_System (last visited Nov 14, 2023).

[44] IT ACT 2000, Avaiable athttps://cis-india.org/internet-governance/blog/uas-license-agreement-amendment (last visited Nov 14, 2023).

[45] IT ACT 2000, Avaiable at https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about (last visited Nov 14, 2023).

any oversight by the Courts or Parliament. Tapping is a serious invasion of an individual's privacy as held in **"*People's Union of Civil Liberties ... vs Union of India and Anr*"[46].**

Senior Internet researchers feel that the CMS is chilling in view of its reckless and irresponsible use of the sedition and Internet laws. They feel that it may be used to silence critics, journalists and human rights activists. The right to privacy is guaranteed under the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights to which India is a state party. Article 17 of the Covenant provides that:

1. no one shall be subjected to arbitrarily or unlawful interference neither with his privacy, family, home or correspondence nor to unlawful attacks on his honor and reputation;
2. Everyone has the right to the protection of the law against such interference or attacks."[47]

For quite a long time in India there was no law governing cyber laws involving privacy issues, jurisdiction issues, intellectual property rights and a number of other legal issues. To optimize benefits of ICTs and secure confidence of user's information society should be safe and secured not only through cyber laws per se but also appropriate enforcement mechanisms. In order to formulate strict statutory laws to regulate the criminal activities in the cyber world the Indian Parliament passed the ''**Information Technology Act, 2000**" to protect the fields of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cyber-crimes. The Act was further amended in the form of Information Technology Amendment Act, 2008 (ITAA-2008).[48]

**The Aadhaar data breach (2018)**- Aadhaar, which means 'foundation', is a 12 digit unique identity number issued to all Indian residents based on their biometric and demographic data. The Unique Identification Authority of India (UIDAI), a statutory body that oversees the world's largest biometric identity card scheme, following a report in The Tribune[49] that claimed unrestricted access to any Aadaar number for a paltry sum of Rs 500. Biometric data, unlike the UIDAI's statement, is not the only privacy concern with this breach. The disclosure of demographic data, such as an individual's name, date of birth, address, PIN, photo, phone number, e-mail, etc, is not any less of a privacy concern. This data forms the basis of many cybercrimes, be it phishing or identity theft. Additionally, obtaining biometric data is getting simpler, such as the extraction of fingerprints from photographs or the spoofing of iris scans. Obtaining biometric data will be a huge target for cybercriminals, because of the potential of combining it with the troves of other information already illegally available. It is extremely dangerous, therefore, to underestimate the value of the data disclosed in this breach, simply because it did not include biometric data, A data 'breach' is not defined under the Indian Information Technology Act, 2000 or the Aadhaar Act, 2016. However, a data 'breach' is not limited to a technical breach like hacking the security systems of the Central Identities Data Repository (CIDR), as is commonly understood. Gaining unauthorized access to a database – in this case, possibly the CIDR – is very much a data breach and a violation of privacy. It is the seriousness of this act of gaining unauthorized access to the Aadhaar database, which makes it punishable not only under Section 43 of the IT Act but also under Section 38 of the Aadhaar Act itself.

[46] People's Union of Civil Liberties vs Union of India and Anr, AIR 1997 SC 568
[47] Article 17, UDHR, http://www.un.org/en/universal-declaration-human-rights/
[48] IT ACT 2000, Avaiable at http://www.cyberlawtimes.com/category/cyber-laws/ (last visited Nov 14, 2023).

[49] Rachna Khaira, Tribune News Service , http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html (last visited Nov 14, 2023).

It is a relief that the breach did not involve a large amount of data being downloaded and stolen, as was seen in the Equifax data breach, where their grievance redressal system was hacked. Nevertheless, each individual whose number has been entered into the system and details extracted in this case has had his privacy violated. The potential of this breach is much greater, with almost any Aadhaar holder's information being accessible this way. American whistleblower *Edward Snowden*[50] delivered a firm reproof to the Indian government for "destroying the privacy" of its citizens and spoke out in support of the reporter who broke the **Aadhaar data breach**. Government of India has recently decided to introduce an exhaustive law on privacy, which will soon be introduced before the parliament. This law provides for stringent punishment, including revocation of licenses of telecom service providers, for illegally intercepting telephone calls and making their content public. After the Supreme Court declared privacy a fundamental right, it is left to Parliament to define what constitutes privacy under the ambit of right to life and personal liberty. Parliament will also have to define reasonable restrictions in the case of right to privacy as it involves, already pointed out by intelligence agencies, the issues of national security.With these restrictions, defining privacy is going to be big challenge for the parliamentarians.
You cannot define right to privacy in absolute terms. Codification of right to privacy right will be a big problem. It will be a challenge for Parliament to accurately define what constitutes privacy,[51] Another significant step taken by the government of India for ensuring cyber security and controlling cyber-attacks in India is the National Cyber Security Policy 2013, unfortunately the reactions of cyber experts over the policy in terms of privacy protection are not encouraging. The need of incorporating stringent provision in this policy to deal with privacy infringement effectively is expressed by the individuals concerned.

## IMPORTANCE OF DATA PROTECTION AND PRIVACY IN INDIA

Data protection and privacy are crucial in India, as they are globally, due to the increasing digitization of information and the growing reliance on technology. India has emerged as a top choice for global outsourcing (Clutch, 2015). India has clearly benefited from outsourcing. In a survey conducted by Statistic Brain Research Institute (2015), 26% of Chief Financial Officers (CFOs) favor India for their company’s outsourcing needs. The surveyed companies have cited economic, political, and cultural incentives for choosing India. Companies have also been impressed with India’s pro-business and entrepreneurial climate.

India’s historical trade ties to the United Kingdom and United States also play an important role (George and Gaut, 2006). India also possesses low-cost and highly qualified workforce with English speaking capabilities and advance educational standards. India’s steady democratic government, independent institutions, advances in Information Technology as well as convenient geography which is suitable for around the clock work makes it possible for companies to seek outsourcing to India as a preferred destination (Chandra and Narsimhan, 2005).

[50] Edward Snowden is an American computer professional who initially worked with the Central Intelligence Agency and then the National Security Agency before being charged with leaking information about United States Surveillance program to the media.
[51] Prabhash K Dutta, http://indiatoday.intoday.in/story/right-to-privacy-fundamental-rightparliament/1/1032794.html (last visited Nov 14, 2023).

However, it is important to note that the global competition for outsourcing is increasing. Countries like Indonesia, Estonia, Singapore, Indonesia, Bulgaria, Philippines etc. are giving a tough competition to India. Moreover, countries in Europe and United States consider privacy a fundamental right. So, it is a need of the hour that India should toughen its data protection and privacy laws. It is also important that India should encourage the companies to self-regulate. India needs to address the loopholes in its data protection and privacy laws to address the concerns of American and European companies about their data protection and privacy. India needs to assure its outsourcing clients that cost-effectiveness of outsourcing would not be diluted by the additional costs of handling customer data privacy apprehensions, in case of a breach.

## CONCLUSION

The importance of right to privacy for the maintenance of dignity of an individual is beyond explanation. It is paramount in the light of increasing attacks on the privacy over internet to address this issue immediately and adopt stringent measures against these attacks. The solution to the problems lies into the global initiatives and any measure adopted nationally is not likely to produce drastic results. But, still it is necessary to evolve some mechanism by which effective remedy be provided to those who are victimized of privacy violation. The legislative measures are adopted in India in this regard though seem to be enough on paper but when it comes to implementation, lack of awareness amongst the users, the internet habits of the users in India and lack of expertise amongst the enforcement agencies are presenting serious challenges ahead.