VOLUME 4 | ISSUE 4 **MAY 2024** **ISSN: 2582-7340**

VOLUME 4 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

THE RIGHT TO PRIVACY IN THE DIGITAL AGE

- Dr Sumbul Fatima[1]

ABSTRACT

Technology has advanced to great advantage for humanity. But as technology develops, a lot of our freedoms are now in jeopardy. Concern over the right to privacy is growing as technology develops and the amount of data being continuously collected and processed in the market increases. The advent of digitalization has given rise to illicit activities such as identity theft, cyberbullying, and data fraud. Users' private information is typically handled improperly when they provide it to websites for businesses, state agencies, digital networking, interaction intelligence corporations, and others. The constant advancements in technology and electrical systems in today's society provide us with many conveniences that make life easier. Even though some argue that privacy safeguards have gotten better, every new advancement in this field also raises the risks to people's privacy. People are in danger because India does not have a comprehensive law protecting the privacy of personal data. The current IT regulations are inadequate and do not provide enough security. Security cannot be guaranteed, even if someone believes they have taken all the appropriate precautions to protect their personal information. The more people who use the internet, the greater the likelihood that someone will violate someone else's privacy. When someone is debating a purchase, an odd thing happens: social media feeds soon after showing ads for the same products, giving the impression that someone is paying attention. With more people using the internet and disclosing personal information voluntarily, the significance of privacy rights in our daily lives is increasing. The privacy laws that exist now were created without considering the challenges of the current digital era, during a time when telegrams and phone lines were commonly used.

Keywords: *Privacy, Digital era, hacking, arbitrary interference, social media, right to be forgotten*.

[1]Dr. Sumbul Fatima, Assistant Professor, School of Law(SOL), Manav Rachna University, Faridabad, Haryana.

1. 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 connected to, along 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 in August 2017[2] determined that the "Right to Privacy" is a fundamental right even though the Indian Constitution does not specifically recognise it as such.In India, there is currently hardly any data protection legislation or data safeguarding agency despite a plethora of administrative initiatives. Nonetheless, India has made significant progress in acknowledging the right to privacy. The Indian Supreme Court ruled in ***M.P. Sharma v. Satish.***[3] Chandra that the Indian Constitution does not guarantee the right to privacy. The bench was debating whether Article 19(1)(f) of the constitution is violated by a search order 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 Articles 21[6] and 19(1)(d)[7] of the Indian Constitution safeguard the right to privacy as a fundamental right. In the current case, the Court was considering the provisions for continuous surveillance found 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*[8]." The Supreme Court determined that expanding the right to privacy to include telecommunications is a serious violation of an individual's rights[9] while discussing the issue of telephone tapping. Furthermore, the Supreme Court acknowledged the distinction between mental and physical privacy[10]. A person who has been assigned an Aadhar number is not permitted to share their biometric information with any third party without express permission, as per the ruling in the case of ***Unique Identification Authority of India v. Central Bureau of Investigation***[11]**.** Subsequently, the

[2] *K.S. Puttaswamy v. Union of India* MANU/SC/0911/2017.
[3] MANU/SC/0018/1954.
[4] Section 96(1), The Code of Criminal Procedure, 1973.
[5] MANU/SC/0085/1962.
[6] Article 21, The Constitution of India, 1950.
[7] Article 19(1)(d), The Constitution of India, 1950.
[8] *Govind v. State of Madhya Pradesh*, MANU/SC/0119/1975.
[9] *People's Union for Civil Liberties v. Union of India* MANU/SC/0149/1997.
[10] *Selvi v. State of Karnataka,* MANU/SC/0325/2010.
[11] MANU/SC/0374/2017.

landmark decision in ***K.S. Puttaswamy v. Union of India***[12] was rendered, in which the Unique Identity Scheme was evaluated concerning privacy concerns. The Indian Constitution Bench had to determine whether the right to privacy is protected by the Constitution and, if so, where it originates, given that the document lacks a clear framework for privacy.

This ruling clearly concluded that privacy is a fundamental right guaranteed by the Indian Constitution, setting it apart from previous precedents. 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 jurisdictions. Sections 43-A and 72-A of the Information Technology Act[13]were particular provisions protect an individual's personal data prior to the "Right to Privacy" being recognized as a fundamental right under Article 21 of the Indian Constitution. The Telegraph Act, of 1885, governed communication interception[14].

The recently enacted Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, imposes requirements on companies who gather information in order to secure private data.[15].

It is believed that humans are autonomous creatures with an innate need for privacy and control over specific areas of their lives. Human behavior has an innate and inalienable need for privacy, which is now acknowledged as a fundamental human right. Since each person's privacy is an essential component of their life and freedom, it must be safeguarded. The importance of this right to privacy has been acknowledged on occasion by academics and judges, and it currently occupies a unique place in contemporary life. The right to privacy is not explicitly stated in the Indian Constitution; rather, it was included in the category of fundamental rights through the use of judicial interpretation. Man has become more sensitive to publicity due to the intensity and complexity of the advancing civilization, which makes privacy and solitude increasingly important for an individual. However, as society has advanced, modern companies have found several products that violate privacy. We live in an era of information technology right now. A new world with faster information sharing, greater transparency, and improved communication has emerged as a result of the internet's expansion and evolution. But everything has advantages and disadvantages. Rapid technological advancement is inevitably accompanied by an

[12]Supra Note 1.
[13]Section 43-A and 72-A, The Information Technology Act,2000
[14]Section 5 & 24, The Telegraph Act, 1885
[15]Replaced Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Rules), 2011.

increase in misuse, which is made worse by the growing use of the Internet for the sharing of private, sensitive, and commercial information. There are limits to privacy, and it isn't always perfect. The relevant state authorities have passed a number of laws to protect citizens' privacy, but these measures are not unrestricted and are subject to limitations in some areas. However, as more information is shared online and more data is converted to digital form, privacy is becoming increasingly important. People have a great deal at stake when it comes to the privacy of their information, so data regulations must take that into consideration. This essay will examine how the development of technology can impact a person's life and freedom, with a focus on privacy as a crucial element. We will also talk about the new areas that the digital age of technology has created where people's privacy needs to be protected and how much it needs to be protected. The study will also include an overview of how the government has managed data privacy through various laws and regulations.

2. Privacy in the Digital Age

Any information is accessible with only a few clicks in this day and age of information. There are many benefits to the explosion of information, but there are drawbacks as well. The amount of data generated by different electronic devices and applications has increased significantly over the past ten years. Data is generated and is all around us in almost everything we do.

There are two types of information: the first is the information we voluntarily share, and the second is information that is created literally every time we take a step, like using a transportation system, ordering food, or traveling. Without a doubt, in this era of ubiquitous internet access, such information has become extremely valuable and has a newfound value. Many large corporations assess the data from this information and use it to inform their business strategy decisions[16]. Privacy needs to be protected because this access to information is something that people might not want to provide. Both non-state entities and the state are challenged on the grounds of the right to privacy.

Privacy Concerns Against the State: States are using technology in the most creative ways possible, especially in light of the rise in international terrorist attacks and the increased concern for public safety. One such method that States are using is profiling, which is the automated processing of personal data to assess certain personal characteristics of an individual, specifically to analyze or forecast aspects related to that individual's work performance, financial status, health, preferences, interests,

[16] Data Protection & Privacy Issues in India, Economic Law Practice 2017, September 01, 2017, available at www.eplaw.in (last accessed on September 06, 2023

dependability, behavior, location, or movements.[17]. Discrimination on the basis of caste, religion, and ethnicity may arise from such profiling.

However, profiling can also be employed to protect national security and advance public interest. The security landscape in our nation and around the world forces the State's and people's safety to be weighed against this right to privacy.

Each time someone clicks on something on the internet, data is created both actively and passively. It has been noted that Uber is aware of our whereabouts and the locations we frequently visit, Facebook, at the very least, is aware of our friendships, Alibaba is aware of our purchasing patterns, and Airbnb is aware of our travel plans.[18]. Non-state actors that possess extensive knowledge of our movements, financial transactions, personal and professional conversations, health, mental state, interests, travel locations, fares, and shopping habits include social network providers, search engines, email service providers, and messaging applications.

Therefore, it is necessary to protect the information that users are unwilling to share. Legislative intervention and appropriate state action are needed to protect user privacy and establish the bounds of what can be inadvertently compromised. It is, therefore, reasonable to argue that the current state of affairs places restrictions on the authority of the government and other non-state actors in order to protect citizens' right to privacy.[19].

2.1. Current Techno-Legal Protection

The right to privacy is now recognized as a fundamental freedom, an integral component of Article 21—which safeguards citizens' lives and liberties—and one of the rights enumerated in Part III of the Constitution. In the historic case of Justice ***K.S. Puttaswamy v. Union of India***[20], a nine-judge panel rendered a unanimous decision on August 24, 2017, reaffirming that every Indian citizen is entitled to a fundamental right to privacy under the country's constitution.

India hasn't yet passed any particular data protection laws, though. The Information Technology Act of 2000 and the Information Technology (Reasonable Security Practices and Procedures and

[17] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[18] Tom Goodwin, The Battle is for customer interface, March 03, 2015, available at https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle- is- all-for-the- customer-interface/ (last accessed on April 06, 2021)

[19] Daniel Solove, 10 Reasons Why Privacy Matters, January 20, 2014, available at http://www.teachprivacy.com/10-reasons-privacy-matters/ (last accessed on April 06, 2021)

[20] (2017) 10 SCC 1

Sensitive Personal Information) Rules, 2011 (commonly referred to as IT Rules) are the main laws pertaining to data protection. Additional requirements regarding the gathering and sharing of sensitive personal data or information were placed on commercial and business entities in India by the IT Rules.

It contained a number of new regulations requiring businesses and organizations that handle personal data to get the written consent of the data owner before doing certain tasks. Sections 43A and 72A were added to the IT Act of 2000, along with other changes brought about by the Information Technology (Amendment) Act of 2008.In addition to providing compensation to the person harmed by wrongful gain or loss, Section 43A addresses the application of reasonable security practices for sensitive personal data or information[21].

Passwords, financial information (such as bank account or credit card details), physical, physiological, and mental health conditions, sexual orientation, medical records and history, and biometric information are among the categories of sensitive personal data or information mentioned in the provision. A person who discloses another person's personal information while performing services in accordance with the terms of a valid contract[22]Faces up to three years in prison and/or a fine of up to Rs. five million. This is known as Section 72A.

According to Rule 5 of the IT Rules, 2011, no body corporate or person acting on its behalf may gather any personal data or information unless it is legally required for any function of the body corporate and the information collection is required for that purpose. The person whose information is shared also needs to be informed about the information being collected, why it is being collected, who the intended recipients of the information are, and the name and other specifics of the agency that is collecting and keeping the data. Any corporate entity or individual in possession of a data subject's personal information is not permitted to keep it for longer than is necessary under law or to use it for purposes other than those for which it was originally obtained. The information source may choose to consent to the collection of data or not, and they may also revoke their prior consent at any time. Even in order to share information with third parties, consent is necessary.

However, when information is shared with government agencies required by law to obtain information—including sensitive personal data or information for identity verification—or for the purposes of prevention, detection, investigation, including cyber incidents, prosecution, and punishment of offenses, such consent from the information provider is not necessary.[23].

[21] The Information Technology Act, 2000, s 43A
[22] The Information Technology Act, 2000, s 43A
[23] The Information Technology Act, 2000, s 72A

These regulations, however, only address the gathering and sharing of data by a corporate entity. Sensitive personal data or information is not thought to include information that is publicly accessible. There is no comprehensive legislation in the Indian legal system that governs the gathering and sharing of personal information. The processing of personal data that is not specifically sensitive personal data or information is not subject to any particular regulations.

Personal Data Protection Bill, 2019: A Committee of Experts headed by Justice B. N. Srikrishna was established in July 2017 to look into a number of data protection-related issues in India. In July 2018, the Committee delivered a draft Personal Data Protection Bill 2018 and its report to the Ministry of Electronics and Information Technology. The Minister of Electronics and Information Technology introduced the Personal Data Protection Bill 2019 in the Lok Sabha on December 11, 2019.

This Bill's objectives are to protect people's privacy with regard to their personal data and to create an Indian Data Protection Authority to handle these and other issues pertaining to personal data.[24].The bill aims to regulate the handling of personal information that has been gathered, shared, disclosed, or otherwise processed inside the borders of India:

- By the government, any Indian Company, any citizen of India, or any person or body of persons incorporated in India, and
- International businesses that handle the personal information of Indian citizens. Since it was introduced in the Lok Sabha, the bill has been referred to a Joint Parliamentary Committee, which is anticipated to report on it during the upcoming monsoon session.

2.3. Whatsapp-Facebook Privacy Issue: Many service providers operate in India to facilitate communication through sharing media and other data, as well as having private conversations. One such smartphone app that is highly used in India is WhatsApp. Whatsapp was first launched in 2010 and was purchased by Facebook, a multinational technology company, in 2014 with the assurance that its privacy policies would not alter.

2016 saw the announcement of changes to WhatsApp's privacy policy, which included sharing user account information with Facebook. Following the Delhi High Court's ruling allowing information shared via WhatsApp to be accessed under its new privacy policy, a petition was filed with the Supreme Court challenging this altered privacy policy on the grounds that it violated users' right to privacy[25].

[24] Anurag Vaishnav, "The Personal Data Protection Bill, 2019: All you need to know, The PRS Blog, December 23, 2019, available at https://www.prsindia.org/theprsblog/personal-data-protection-bill-2019-all-you-need-know (last accessed on April 07, 2021

However, the Court ordered WhatsApp to remove the data of users who decide to remove the application from their phones as well as users who choose to keep it installed until September 25, 2016[26]. The new privacy policy was challenged in February 2021 in the ***Karmanya Sareen v. Union of India.***[27]Case. The application argued that the privacy protection standards in India are far lower than those in European countries, effectively discriminating against the country's Indian users. The parties have been notified by the Supreme Court and requested to submit their responses.

WhatsApp has extended its update deadline until May 15, 2021, in response to harsh criticism. An **Indian Chief Justice**, **SA Bobde**, along with **Justices AS Bopanna** and **V Ramasubramanian,** comprise the three-judge bench that is considering the case.

3. Conclusion

The right moment was right for the Court to examine the right to privacy. The adoption of electronic governance has started in India. Web connection statistics show that public interest in information technology-based procedures is changing. In light of this, a privacy ombudsman might be a useful tool to make sure the government doesn't abuse its power while the legislature works to enact specific legislation governing this kind of right. Similar processes are followed in the United Kingdom, where a court called the Investigatory Powers Tribunal is in charge of limiting the state's surveillance powers and ensuring that no one's right to privacy is infringed. A court may also mandate an evidence-based decryption procedure. According to this strategy, the law enforcement agency must present sufficient corroboration to the courts in an effort to convince them that decryption is necessary.

One of our fundamental rights is the right to privacy. It is a right that grants people the freedom to make independent decisions about their lives while shielding their inner selves from interference from both state and non-state entities. One can accurately say that technology has made it possible for both State and non-state actors to enter a citizen's home without knocking on the door. An individual has the freedom to choose who lives with him, who he associates with, and in what kind of relationship.

[25] Angelina Talukdar, India: Key Features of The Personal Data Protection Bill, 2019, March 16, 2020, available at https://www.mondaq.com/india/data-protection/904330/key-features-of-the-personal-data-protection-bill-2019 (last accessed on April 07, 2021)

[26] Karmanya Singh Sareen v. Union of India, SLP (C) 804/2017

[27]Whatsapp Facebook Privacy, by Supreme Court Observer, available at https://www.scobserver.in/court-case/whatsapp-facebook-privacy-case (last accessed on April 10, 2021)

The family, marriage, procreation, and sexual orientation—all significant facets of dignity—must be safeguarded by the privacy of the home. It does not follow that others can enter the house just because the owner allows someone else to. The only safeguard is that it shouldn't injure the other person or interfere with their rights.

This holds true for both technology and the material world. In a time when social and cultural norms are numerous and diverse, especially in a nation like ours that values its diversity, privacy is one of the most crucial rights to be safeguarded against both State and non-state actors and to be acknowledged as a fundamental one. The necessary steps should be taken by the legislature to guarantee that the privacy of its people is protected.

Few things, like national security, etc., are more important than people's right to privacy, which supports the idea that privacy is a right with some legitimate limitations. It is hoped that when the pending Personal Data Protection Bill comes into effect, it will close the current gap between the legal system and technology. Advanced technology demands more advanced laws.

India is continuing to uphold the measures that safeguard national security while simultaneously pursuing a more user-privacy friendly legal framework. The country can take cues from other countries and create a more robust framework that would entice several digital behemoths to choose India as their home country. This will help India reach its objective of developing an economy valued at five trillion dollars.