International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

A Comprehensive Analysis on Right to Privacy in the Digital Age under the Ambit of Data Privacy Laws in India

Vaishanvi Anand

BBA LL.B 3RD Semester, Amity Law School, Amity University Patna, Patna, Bihar, India

Abstract: ***Researching the engrossing reasons behind the contravention of right to privacy in the era of amplification of technology in IT ACT and is inherently protected under Article 21 as a part of freedoms guaranteed by Part III of the Indian Constitution, a thorough analysis on the advance realms of technology and technology can affect the life of an individual with their privacy at its most important component. The principal objective of this research is to study the new opportunities have arisen to safeguard the privacy of individuals, prompting a consideration of the extent to which it should be preserved. This research also comprehends that how government has addressed data privacy through the implementation of diverse laws and regulations.***

Keywords: Right to privacy, IT{Information technology} Act, Article 21, cyber crimes

1. Introduction

Privacy is not always feasible and is issue to specific constraints. Various laws enacted by authorities aim to safeguard the privacy of an individuals, yet these protections are not absolute and are circumscribed by the government in specific domains. With the increasing digitization of data and the surge in online information exchange, there is a growing emphasis on privacy. The regulation of data becomes crucial, considering its perceived significance, given that individuals have much at stake concerning the confidentiality of their information. The more and more technology being evolved the more privacy slips away.

Even in India, the right to privacy is not explicit in the Indian constitution, it was incorporated under the realms of fundamental rights under the judicial interpretation. The intensity and complexity of advancing enlightenment have made an individual more sensitized towards publicity, making seclusion and privacy more essential for an individual.

1.1 Constitutional provision under Article 21

The “right to privacy,” or the right to be let alone is guaranteed by Art.21 of the constitution. A citizen has a right to safeguard the privacy of his own, his Family, Marriage, procreation, motherhood, childbearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right of a person concerned and would be liable in an action for damages. However, position may be differed if he voluntarily puts into controversy or voluntarily invites or raises a controversy.

Indian Constitutional statute has been witnessed post-Mrs Gandhi’s case. In numerous court cases, it has been asserted that the essence of Fundamental Rights in India is encapsulated in Article 21. Therefore, it can be affirmed that Article 21 possesses multidimensional aspects. The scope of Article 21 has expanded, giving particular significance to the terms "Life" and "Freedom," both of which require precise interpretation. The Right to Privacy is an exemplar of a right that has found its foundation in the broadening scope of Article 21. While the constitution does not explicitly grant a right to privacy, the Supreme Court has discerned various rights within the ambit of Article 21. According to Black's Law Dictionary, Article 21 of the Indian Constitution stipulates that "No person shall be deprived of his life or personal liberty except according to procedure established by law."

The right to privacy is not explicitly recognized as a Fundamental Right in the Indian Constitution. The initial exploration of this issue emerged in the Kharak Singh case, which raised concerns about the legality of specific directives allowing surveillance of respondents. This privilege is the right to remain unmentioned. Concerning surveillance, it has been established that if intrusive and genuinely infringing on a citizen's privacy, it can impinge on the freedom of movement guaranteed by Articles 19(1)(d) and 21. Article 21 of the Indian Constitution, which addresses the right to life, has been expansively interpreted to encompass more than mere survival, incorporating aspects that make a person's life more meaningful, complete, and worth living. The right to privacy is recognized as one such aspect of this right to life and personal liberty.

The Kharak Singh v. Province of UP case marked the first instance where the issue of the right to privacy was raised. The Supreme Court ruled that Regulation 236 of the UP Police directive was illegal as it contravened Article 21 of the Constitution. The Court affirmed that the right to privacy is a component of the right to the protection of life and personal liberty, equating "privacy to personal liberty."

In the Maneka Gandhi case, a triple test was established for any law interfering with personal freedom:

- it must prescribe a procedure;

- the procedure must withstand the test of at least one of the fundamental rights provided under Article 19, relevant in each situation; and
- it must withstand the test of Article 14. The law and procedure allowing interference with an individual's freedom and right to privacy must also be correct, fair, rational, and not arbitrary, whimsical, or oppressive.

In the Naz Foundation Case of 2009, the Delhi High Court examined consensual homosexuality, evaluating Section 377 of the Indian Penal Code and Articles 14, 19, and 21. The court held that the right to privacy ensures a "privacy in which a man may become and remain himself."

2. Research Methodology

The researcher will primarily focus on analysing and studying the contraventions of right to privacy in the era of amplifications of technology of IT {information technology} act, 2000, a through analysis on the advance realsm of technology and how technology can affect the life of an individual with the privacy as the most important component. The study involves a diligent study about the contravention of the technology.

2.1 Privacy Rights in the Digital Era

The establishment of privacy law standards for the digital media was imperative due to the voluminous and easily transferable nature of information in digital form. The contemporary landscape witnessed the accumulation of extensive data by individuals and corporate entities for various purposes. This concern was articulated by Justice Douglas in Sampson v. Murray, where he expressed, "With dossiers being compiled by bureaus, state and local law enforcement agencies, the CIA, FBI, IRS, the Armed Services, and Census Bureau, we live in an Orwellian age in which the computer has become the 'heart of a surveillance system that will turn society into a transparent world.'"

Justice Douglas's statement had the effect of applying George Orwell's "Big Brother" theory to the digital realm, wherein he perceived the gathering of vast amounts of information as a potential threat.

Both in India and in UK law, data protection laws tend to regulate databases. The legislations in both countries follow a similar "consent purpose" model derived from the principle of law of confidence developed in the UK. This model stipulates that personal data should be collected for specific purposes only with an individual's consent, and the collected information should not be used for any other purposes than those to which the individual agreed. The disclosure of personal information to another party for a specific purpose, under the law of confidence, is akin to consenting to the use of the disclosed information by that party for such a purpose. This model is also reflected in the "Rules on the Protection of Privacy and Transborder Flows of Personal Data" issued by the Organization for Economic Cooperation and Development (OECD).

The Law of Confidence initially evolved in England concerning trade secrets. It appears reasonable that imposing an obligation on the recipient of information to use the data only for the disclosed purpose, especially when it is revealed for a restricted object, is well-suited to safeguard trade secrets. In the United States, the law of confidence primarily developed in the medical context. One of the earliest cases on the law of confidence, Simonsen v. Swenson, was related to information disclosed by a patient to her doctor.

The current era is characterized by the prevalence of information technology. The evolution of the internet, along with its widespread accessibility, has ushered in a new world marked by improved communication, faster information sharing, and enhanced transparency. However, every development has its advantages and disadvantages. The rapid progress in technology is accompanied by a rise in its misuse, a phenomenon largely unavoidable and exacerbated by the expanding use of the internet for the exchange of sensitive, private, and commercial information.

There are two types of information: one that individuals willingly share, and the other that is generated automatically through various activities such as travel, meal orders, or transportation usage. Undoubtedly, this information holds significant value and has become a new form of currency in the age of widespread internet access. Many large companies analyse data from these sources and incorporate it into their business strategies. The access to information, especially that which individuals may not intend to disclose, requires the protection of privacy. The right to privacy is asserted not only against the state but also against non-state actors.

The increasing digitization of our lives is undeniable. The transformation brought about by technology extends across our communication with friends and family, our work habits, and even our shopping practices. In tandem with this shift towards a more digital existence, our considerations regarding privacy have also undergone significant changes. While personal information was traditionally confined to physical forms such as paper documents or home movies, it is now predominantly stored online. This transition has facilitated unauthorized access to our information, be it through hacking into email accounts or companies collecting data for marketing purposes. In the digital age, our privacy faces constant threats and challenges.

In the digital age, one of the most significant threats to privacy rights is the extensive collection of data by internet companies. These entities amass vast quantities of user data, ranging from browsing histories and search queries to location and demographic information. Subsequently, this data is utilized for targeted advertising and various other purposes. Notably, even if an online user is not actively logged into a specific service, their data may still be gathered and utilized.

Another formidable challenge to privacy rights is the prevalence of online harassment. The anonymity afforded by the internet allows individuals to engage in behaviour they might never consider in face-to-face interactions. This includes activities such as making threats of violence, engaging in sexual harassment, cyberbullying, and other forms of cyber-attacks. Victims of online harassment often

encounter difficulties in halting such behaviour as perpetrators can be challenging to identify and track down.

2.2 Sources of Data and information

The incorporation of a diverse array of secondary data sources, such as books, newspapers, and legal articles, played a pivotal role in attaining a comprehensive understanding of the subject under consideration. These sources offered valuable insights and diverse perspectives that might have been overlooked otherwise. The utilization of secondary data sources proved instrumental in amassing a substantial amount of information.

United Kingdom

In the United Kingdom, the handling of data in digital form is governed by the same principles established for traditional forms. Under the Data Protection Act 1998, the term "Data Controller" refers to the individual who determines the reasons and methods for processing data, either alone or jointly with others. The Act outlines six principles of data protection and security, summarized as follows:

1) First guideline: Ensuring the fair and legal processing of information.
2) Second guideline: Collecting data for specific and legal purposes.
3) Third guideline: Data controllers should retain information that is adequate, relevant, and not excessive concerning the purpose of collection.
4) Fourth guideline: Ensuring that all information is accurate and up-to-date.
5) Fifth guideline: Personal information should not be retained for longer than necessary.
6) Sixth guideline: Processing data in accordance with the rights of information subjects under the Act.

These principles emphasize the importance of fair and lawful handling of data, the necessity for collecting data for specific and legitimate purposes, and the need to ensure that data held is adequate and relevant. Additionally, accuracy, currency, and the appropriate retention period for personal information are highlighted to safeguard the privacy and rights of individuals under the Data Protection Act.

In the United Kingdom, for the collection and processing of "sensitive personal data" as defined under Section 2 of the Data Protection Act, adherence to one of the eight conditions specified in Schedule III of the Act is mandatory. Among these conditions, obtaining the consent of the data subject is one of the approved methods. Therefore, if any of the other conditions or situations outlined in Schedule III are not applicable, the consent of the data subject must be obtained for the collection and processing of sensitive personal data.

India

Section 43 of the IT Act prohibits unauthorized access to information from another person's computer without their consent, addressing the "intrusion upon seclusion" aspect of privacy breach as proposed by Prosser.

Section 43A, introduced by the IT Amendment Act of 2008, deals specifically with sensitive personal information. The Central government, empowered by this provision, issued the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, commonly known as the IT Rules. These rules define 'sensitive personal data' and mandate that the 'body corporate or any individual who, on behalf of the body corporate' collects sensitive personal data must provide a "privacy policy" to the information provider. This policy informs the provider, among other things, about the purpose for which the data is being collected.

Rule 5 of the IT Rules integrates and underscores the principles of data protection embodied in the English Data Protection Act 1998. Schedule VI of the IT Rules contains a detailed prohibition against the disclosure of sensitive personal information to third parties without the consent of the data provider. This legal framework aims to ensure the security and confidentiality of sensitive personal information, aligning with international data protection principles.

Current techno-legal Protection

The right to privacy has been established as a fundamental right and an inherent part of Article 21, protecting the life and liberty of citizens as part of the freedoms guaranteed by Part III of the Indian Constitution. This landmark decision was made in the case of Justice **K.S. Puttaswamy v. Union of India** in 2017, where a nine-judge bench unanimously affirmed that the Constitution guarantees every individual a fundamental right to privacy.

Despite the recognition of the right to privacy, India has not enacted specific legislation on data protection. The primary laws addressing data protection are the Information Technology Act, 2000, and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011, commonly known as the "IT Rules." These rules impose additional requirements on commercial entities in India related to the collection and disclosure of sensitive personal data.

The IT Rules introduced various provisions requiring companies to obtain the written consent of data owners before undertaking certain activities involving personal information. **Section 43A**, added by the Information Technology (Amendment) Act, 2008, addresses the implementation of reasonable security practices for sensitive personal data, providing for compensation to individuals affected by wrongful loss or gain.

The term "sensitive personal data or information" includes passwords, financial information, health conditions, sexual orientation, and biometric information. Section 72A of the IT Act prescribes penalties for the wrongful disclosure of personal information.

Rule 5 of the IT Rules stipulates that anybody corporate or person collecting personal data must do so for a legal purpose related to the corporate body's functional activity. The data subject must be made aware of the collection, purpose, intended recipients, and details of the agency collecting and retaining the information. Consent is required for sharing information with third parties, except when mandated by law for government agencies.

However, these regulations only apply to corporate bodies collecting and disseminating data, excluding information freely available in the public domain. The lack of comprehensive legislation to regulate the collection and dissemination of non-sensitive personal data is a notable gap in the Indian legal system.

The Personal Data Protection Bill, 2019, aims to address these gaps and was introduced to provide protection to individuals' privacy concerning their personal data. The bill is currently under consideration by a Joint Parliamentary Committee, which is expected to submit its report in an upcoming session.

The WhatsApp-Facebook privacy issue highlights challenges in data protection. WhatsApp's changes in privacy policy, particularly sharing user information with Facebook, led to legal challenges. The Supreme Court directed WhatsApp to delete data until a certain date for users choosing to delete the application. The new privacy policy introduced in 2021 faced criticism, leading to legal challenges based on privacy protection standards in India compared to European countries. WhatsApp extended the deadline for users to update their privacy settings, and the matter is currently being addressed by the Supreme Court.

3. Conclusion

The right to privacy is acknowledged as a fundamental right, serving as a safeguard for the personal sphere of individuals against intrusion from both State and non-State entities. This right enables individuals to make autonomous decisions about their lives, reflecting the notion that technology has the potential to breach a citizen's privacy without conventional boundaries. This intrusion can occur from both governmental and non-governmental actors.

The right to privacy is compared to the sanctity of one's home, emphasizing that an individual has the autonomy to decide who enters their dwelling and to shape their personal life, relationships, family, marriage, procreation, and sexual orientation. Granting permission to one person to enter does not extend permission to others, with the caveat that such actions should not harm others or infringe upon their rights.

This principle is applicable to both physical and technological domains. In a world characterized by diverse social and cultural norms, particularly in a country like India that celebrates its diversity, the protection of privacy emerges as a crucial right against both State and non-State actors. It is imperative for the legislature to enact measures to ensure the preservation of citizens' privacy and recognize it as a fundamental right.

While privacy is considered a fundamental right, it is not absolute and may be subject to reasonable restrictions, particularly in cases involving national security. The evolving landscape of advanced technology necessitates corresponding advancements in legal frameworks. The pending Personal Data Protection Bill is anticipated to bridge the existing gap between technology and the legal system when enacted, ensuring a more comprehensive protection of privacy rights in the digital age.

References

[1] Data Protection & Privacy Issues in India, Economic Law Practice 2017, September 01, 2017, available at www.eplaw.in (last accessed on April 06, 2021
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[3] 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)
[4] 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)
[5] (2017) 10 SCC 1
[6] Data Protection & Privacy Issues in India, Economic Law Practice 2017, September 01, 2017, available at www.eplaw.in (last accessed on April 06, 2021
[7] 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)
[8] 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)
[9] 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)
[10] (2017) 10 SCC 1