Journal of Advances and Scholarly Researches in Allied Education
Vol. XI, Issue No. 22, July-2016, ISSN 2230-7540

Laws to Protect Right to Privacy in the Internet Era

Dr. Aradhana Parmar*

Dean, Faculty of Law, Maharishi Arvind University, Jaipur-302041 (Rajasthan)

Abstract – The purpose of this essay is to reflect on the notion of right to privacy in India and to concentrate on different aspects of it. In India's Constitution, the right to privacy has been seen as an unarticulated basic right. Changes in the country's technological, political, social, and economic landscape demand the acknowledgment of new rights. The law evolves in response to societal developments. One such right that has emerged as a result of expanding the scope of Article 21 is the right to privacy. Despite the fact that the Supreme Court has declared this right to be a basic right under Article 21 of the Constitution and various other sections of the Constitution read in conjunction with the Directive Principles of State Policy, it is not absolute. Because it is an integral aspect of life and personal liberty, the rising infringement of this right by the state on spurious grounds has prompted the Indian judiciary to take a proactive role in safeguarding it.

This article has examined many concerns and challenges in the technological age in terms of privacy regulations, with a focus on UIDAI, Data Protection in the Telecom Sector, Cyber Privacy, and Real-Time Tracking, among other topics. The report finishes by outlining the activities and actions that may be performed to address the aforementioned issues. It will focus on the areas where the government must pay the greatest attention in order to protect individual rights.

Key Words – Fundamental Right, Right to Privacy, Technology, Cyber Privacy, Constitution of India, Supreme court, Information Technology.

----------X----------

1. INTRODUCTION

We now live in a time when we no longer have to wait in large lines in front of banks for financial services, and we can have any item delivered to our home after placing an online purchase. That is the benefit of information technology. With the advancement of the internet and its expansion in accessibility, we are seeing the emergence of a new world in which communication, accessibility, information exchange, and transparency are all improved. But, as the saying goes, there are some drawbacks to every benefit. With the advancement of technology comes an increase in its abuse, which is generally unavoidable, especially given the growing usage of the internet for the interchange of sensitive, private, and commercial information.

At all times, privacy was an important aspect of human existence. However, as more data is digitised and more information is shared online, data privacy is becoming more important. Data privacy relates to how data is managed according to its perceived importance. It's not only a business problem; when it comes to their personal information's privacy, consumers have a lot on the line.

Privacy is not always absolute and is subject to various constraints. Several laws have been enacted by concerned state authorities to preserve their people' privacy, however these protections are not absolute and are restricted by the government in some areas. However, as more data is digitised and more information is transferred online, privacy is becoming more important. People have a lot riding on the privacy of their information, thus data must be managed according to its perceived importance.

"Privacy" is a famously difficult notion to describe, and it is impossible to comprehend as a static and one-dimensional idea. It can only be seen as a collection of rights. 4 It's necessary to comprehend what "Right to Privacy" implies in order to grasp the notion of privacy invasion and the influence of technology on privacy. "The situation or state of being free from public attention to intrusion into or interference with one's conduct or choices," according to Black's Law Dictionary5, which translates to "the right to be left alone; the right of a person to be free from any undue notoriety; the right to survive."

The Indian Constitution does not recognise privacy as a fundamental right. The breadth of this first arose in the case of Kharak Singh, which raised concerns about the constitutionality of detailed orders that permitted responses to be tracked.

This is a luxury that should not be overlooked. In the case of reconnaissance, it has been decided that meddling and really infringing on resident protection may intrude on the possibility for growth guaranteed by Articles 19(1)(d) and 21. "As of now, we've discussed Article 21 of India's Constitution3. Article 21's prized right to life has been liberally interpreted to entail anything more than small survival and insignificant existence or creature presence. It so embraces all of those aspects of life that make a man's existence more significant, complete, and worthwhile to live, and the right to security is one such right. The first time this issue was raised was in the case of Kharak Singh v. Province of UP 4, in which the Supreme Court ruled that Regulation 236 of the UP Police Direction was unconstitutional because it violated Article 21 of the Constitution. The Court determined that the right to security is a component of ideal for ensuring life and individual liberty. The Court has made a comparison between "security and individual liberty" in this case.

It is now widely accepted that article 21's right to life and liberty includes the right to privacy. "The right to privacy is a luxury that should not be overlooked." A resident has the right to protect his or her individual privacy, as well as the privacy of his or her family, marriage, multiplication, parenting, child behaviour, and training, among other things. Anyone who distributes anything about the aforementioned topics without the individual's consent is putting themselves in danger in real life. If a guy deliberately throws himself into conflict or purposefully encourages or provokes a discussion, his position will be distinctive.

"We can trace "right to privacy" emanating from the two expressions of the Preamble, namely, "liberty of thought, expression, belief, faith, and worship" and "Fraternity assuring the dignity of the individual," and also emanating from Article 19 (1)(a)which gives to every citizen "a freedom of speech and expression," and further emanating from Article 19(1)(d)which gives to every citizen "a freedom of speech and expression," and Indeed, the right to privacy is embedded in each of these manifestations and flows from them in tandem".The right to privacy is the ability to be alone or to be free of character assault or abuse. The right to privacy is the right to be free of unwelcome advertisement, to live in solitude, and to be free of undue public intrusion into things that are not necessarily of public importance.

This is true of both the physical and technological forms. Privacy is one of the most crucial rights to be protected both against State and non-State actors and to be recognised as a fundamental right in an era where there are many different social and cultural standards, especially in a society like ours that prides itself on its variety. The legislature should take the necessary steps to ensure that citizens' privacy is protected.Only a few things, such as national security, outweigh the importance of an individual's privacy, justifying the notion that privacy is not an absolute right but is subject to some acceptable limitations. Advanced technology necessitates more advanced regulations, and it is believed that if enacted, the forthcoming Personal Data Protection Bill will bridge the gap between technology and the legal system.

Everything in India is now connected to the Internet, thanks to the growth of the Internet business. Because everything is connected to the Internet, and especially on sites like Facebook, Twitter, Instagram, Linkedin, Google+, and many more sites, all of our personal information can be shared with others, there is a clear need for privacy legislation. Our credit card, debit card, or net banking information is maintained on sites like Paytm, Paypal, and Mobikwick, which can be a hazard because anything can be hacked on these sites. All of this demonstrates the pressing need for a Right to Privacy in the digital age. The requirement of the hour in the Indian legislative landscape is For the appropriate implementation of this right, a right to privacy act must be implemented. Although the current government recognises it as a fundamental right, legislators must implement such judicial precedence in a legislative act.

We call on the UN High Commissioner for Human Rights and the international community to enact accountability measures that ensure privacy invasions are monitored in accordance with international standards. Governments that conduct indiscriminate mass surveillance must be chastised, and their ability to gather and use private information about individuals must be limited. Companies and individuals that steal our data or exploit it for nefarious purposes must be punished. While there are solid utilitarian reasons to allow minimal surveillance in order to implement protective and punishing laws against horrendous criminal activity, we must not allow individuals to become slaves of an authoritarian system like George Orwell's Big Brother.

2. PRIVACY RIGHTS

Rights, according to Salmond, are interests that are safeguarded by 'laws of right,' or moral or legal principles. When moral interests are worth safeguarding, regardless of whether or not there is a legal system in place or the functioning of the law, they are referred to as natural rights. As a result, Roscoe Pound defines natural law as a theory of moral attributes inherent in humans, and natural rights as deductions from human nature established by reason.

The right to privacy, which we are discussing here, obviously qualifies as an inalienable natural right, inextricably linked to two ideals whose preservation is a matter of universal moral agreement: man's inherent dignity and autonomy. The right to privacy is a legal

concept that has been used in numerous legal systems to limit government and private acts that infringe on people's privacy.

The right to privacy may take several forms, beginning with 'the right to be left alone,' as defined by Samuel Warren and Louis D. Brandeis in their famous essay published in the Harvard Law Review on December 15, 1890.

So that we might obtain these distinguishing characteristics of the right to privacy,

(i) The right to privacy refers to the ability to be alone. It's a typical spin on a negative right, where other people are obligated to stay out of your business.

(ii) The right to privacy is an in rem right. The right exists in opposition to the rest of the world.

(iii) A person's inviolate individuality includes the right to privacy.

3. THE EVOLUTION OF INDIA'S RIGHT TO PRIVACY

It is a fallacy to believe that the concept of a supervening spirit of justice appearing in many ways to cure the ills of a new epoch is foreign to Indian history. Even in India's ancient and holy scriptures, there is evidence of a well-developed feeling of seclusion.

Views of Sanjay Kishan Kaul J in a landmark case on the right to privacy.

"परित्राणायसाधूनां विनाशायचदुष्कृताम्।
धर्मसंस्थापनार्थाय सम्भवामि युगे युगे ॥"

The meaning of this profound statement, when evaluated after a thousand generations, is this: Each age and each generation brings with it the problems and afflictions of the times, as Lord Shri Krishna revealed in Chapter 4 Text 8 of The Bhagavad Gita. However, that Supreme spirit of Justice presents itself as distinct values in different ages, geographies, and social conditions in order to ensure that certain eternally loved rights and ideals are always protected and preserved. The principles expressed in inter- Alia, Article 14 and 21, which together serve as the heart stones of the Constitution, are an expression of this heavenly 'Brooding spirit of the law,' 'the collective conscience,' and 'the intellect of a future day.'

आयुवित्तं गृहच्छिद्र मन्तमौषध मैथुने ।
दानं मानापमानौ च नंव गोप्यानि कारयेत ॥

According to Hitopadesha, certain subjects (worship, sex, and family matters) should be kept private. The Ramayana appears to have a well-established norm that a lady should not be seen by a male stranger. The Grihya Sutras specify how one should construct one's home in order to protect the seclusion of its occupants and maintain its holiness while performing religious rites, studying the Vedas, or eating. The Arthashastra forbids entering another's home without the permission of the owner.

In southern India, there is still a denomination known as the Ramanuj Sampradaya, whose followers continue to practise neither eating or drinking in the company of others. Peering into other people's homes is also forbidden in Islam. The Hadith makes it immoral to read other people's letters, just as the Fourth Amendment in the United States ensures privacy in one's papers and personal effects. The desire to live without intervening in the affairs of others is found in the text of the Bible in Christianity.It is a personal act to confess one's sins. Our laws recognise religious and societal conventions that affirm privacy, such as the Civil Procedure Code's exemption of a pardanashin lady's appearance in court.

4. RIGHT TO PRIVACY IN INDIAN JURISPRUDENCE

"No individual shall be deprived of his life or personal liberty except pursuant to process provided by law," says Article 21 of the Indian Constitution. On August 24, 2017, the Supreme Court of India held that the right to privacy is a basic right protected by Part III of the Indian Constitution. This law and regulatory choice will have far-reaching consequences. New rules will now be subjected to the same scrutiny as laws that infringe on human liberty are subjected to under Article 21 of the Indian Constitution. The right to privacy is now unmistakably accessible; the question of its contours and bounds remains unique.

There is no comprehensive data protection or privacy regulation in India. In essence, the current laws and policies are sectoral in character. The necessary provisions of the Information Technology Act, 2000 and its regulations currently govern the collecting, processing, and use of' private information' and' delicate private data or information by a corporate body in India, in addition to other sectoral legislation.

In the case of M. P. Sharma and Ors. v Satish Chandra, District Magistrate, Delhi and Ors., where the warrant granted for search and seizure was questioned pursuant to Sections 94 and 96(1) of the Criminal Code of Procedure, the Supreme Court first considered whether the "right to privacy" is a fundamental right. The Supreme Court concluded that the authority to search and seize did not violate any constitutional provisions. The Court also refused

to recognise the right to privacy as a constitutionally protected right in India.

Following that, in Kharak Singh v State of Uttar Pradesh and Ors., the Court considered whether monitoring an accused's home visits at night would be an abuse of the right guaranteed under Article 21 of the Indian Constitution, raising the question of whether Article 21 included the right to privacy. The Supreme Court decided that such monitoring was in fact in violation of Article 21. Furthermore, the majority judges decided that because Article 21 did not clearly provide for a right to privacy, it could not be regarded as a fundamental right.

5. THE RIGHT TO PRIVACY IN THE DIGITAL AGE

The expansion of privacy regulation requirements to sophisticated media was critical, given how much data was stored in digital form and how easily it could be traded and revealed. Furthermore, modern circumstances have seen an increase in the number of people and corporations holding vast amounts of data for various objectives.

Protection rules in both India and the United Kingdom have a propensity to direct databases. The enactments in India and the United Kingdom have a similar "assent rationale" that is derived from the rule of law of certainty produced in the United Kingdom. This model dictates that a man's personal data should only be obtained for certain reasons/purposes with his consent, and that the data gathered should not be used for any purposes other than those for which the individual agreed. Individual data disclosure to another for a specific cause under the law of certainty is equivalent to consenting to that other's use of the data thus disclosed for that specific reason. This model is also included in the Organization for Economic Cooperation and Development's (OECD).

It gives the idea that the Law of Confidentiality was drafted in England to protect trade secrets. Also, it appears logical that requiring the data recipient to promise to using the data for no other purpose, when the data is exposed for that specific restricted object, is the best way to ensure the exchange of insider facts. The law of certainty was formed primarily in the therapeutic environment in the United States10, with Simonsen v. Swenson11 being one of the most well-known examples involving data given by the patient to her expert.

Data is generated not only through active information sharing, but also passively through each internet click. It has been pointed out that Uber knows where we are and where we go, that Facebook knows who we are friends with, that Alibaba knows our shopping patterns, and that Airbnb knows where we are going. Non-state actors that have extensive knowledge of our movements, financial transactions, personal and professional conversations, health, mental state, interest, travel locations, fares, and shopping habits include social network providers, search engines, email service providers, and messaging applications.

6. CURRENT LEGAL AND TECHNOLOGICAL PROTECTION

Now, the right to privacy is a fundamental right and an integral aspect of Article 21 of the Constitution, which safeguards people' lives and liberties, as well as one of the freedoms granted by Part III of the Constitution. On the 24th of August 2017, a nine-judge bench in Justice K.S. Puttaswamy v. Union of India handed down a major decision, declaring that the Indian Constitution provides each individual a basic right to privacy.

The right to privacy is now a fundamental right and an integral part of Article 21 of the Constitution, which protects people's lives and liberties, as well as one of the constitutional freedoms guaranteed in Part III. On August 24, 2017, a nine-judge bench in Justice K.S. Puttaswamy v. Union of India handed down a momentous decision, declaring that each individual has a basic right to privacy under the Indian Constitution.

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 all examples of sensitive personal data or information as defined in the provision. A person who causes unjust damage or gain by exposing personal information of another person while delivering services under the terms of a legitimate contract is subject to imprisonment for up to three years and/or a fine of up to Rs. 5,00,000 under Section 72A.

Any Body Corporate or person acting on its behalf is prohibited from collecting personal data or information unless it is collected for a legal purpose relating to any functional activity of the body corporate and the collection of such information is necessary for that purpose, according to rule 5 of the IT Rules, 2011. Furthermore, the person whose information is shared must be informed that the information is being collected, the purpose for which it is being collected, the intended recipients of such information, the name and other details of the agency collecting the information, and the agency retaining the information.

The goal of this bill is to provide for the protection of individuals' privacy in relation to their personal data, as well as to establish a Data Protection Authority of India for these purposes and matters relating to an individual's personal data. The law intends to apply the following to the processing of personal data gathered, released, exchanged, or otherwise processed on Indian soil:

a) By the government, any Indian company, any Indian citizen, any individual or group of individuals incorporated in India, and

b) foreign companies dealing with personal data of Indian citizens. After being tabled in the Lok Sabha, the bill was submitted to a Joint Parliamentary Committee, which is likely to give its report during the upcoming monsoon session.

In February 2021, an application was made in the matter of Karmanya Sareen v. Union of India, challenging the new privacy policy on the grounds that the privacy protection standards in India are substantially lower than those in European nations, resulting in discrimination against Indian users. The parties have been given notice of the Supreme Court's decision and have been invited to file their responses.

7. GOVERNMENT PROTECTION EFFORTS

Privacy While governments are often vilified for invading our privacy, they also protect our digital rights and have the power to punish those who violate them. Legislation that protects sensitive data is critical, and many countries are failing to keep up with technological advancements that have broadened the scope of digital rights. Governments must preserve privacy while also promoting openness, two goals that may appear to be mutually exclusive but often work in unison. Governments can ensure that citizens are informed about personal data collected about them, as well as display information about what the government does with that data and its own work.

Medical data, for example, is private information that countries frequently safeguard through regulation. Individuals may face discrimination in terms of employment and insurance if this does not happen. A key dilemma raised by the right to privacy is whether people should have access to medical data that reveal genetic predispositions to disease, as this information may not be useful when preventative measures are not available. Governments must discuss the appropriate degrees of privacy and transparency for their citizenry. In democratic countries, voter privacy rights are especially crucial because they ensure the spirit of free choice that underpins elections. Because international disputes between nation-states frequently spill over into digital contexts, cybersecurity is therefore a national duty.

The Canadian Parliament's Privacy Commissioner's Guidelines for Online Consent and Brazil's "Internet Bill of Rights" are two recent instances of government legislation aimed at increasing transparency in privacy practises. Typically, such legislation aims to regulate user permission and provide control over individuals' dealings with internet providers and platforms.

8. CURRENT CONCERNS

The Supreme Court established a three-fold requirement for the state to interfere with basic rights. While the state may interfere to protect the state's legitimate interests:

a) Article 21 of the Constitution expressly requires that there be a legislation in place to justify an intrusion of privacy.

b) (b) The nature and content of the law imposing the restriction must be reasonable under Article 14;

c) The methods used by legislators.

India, in contrast to today's consent-based paradigm, is frequently urged to embrace rights-based information privacy frameworks. Under the consent-based model, once the user's approval has been obtained, the information controller is free to process, use, and share the information with any third party. However, few people are aware of the true consequences of indiscreet data sharing at the time of acceptance. The rights-based model, on the other hand, allows consumers to have greater control over their data while also requiring the data controller to ensure that users' rights are not violated. As a result, clients have more control over their personal information.

The Supreme Court's decision in the preceding cases allows Indian citizens to seek judicial remedies if their data privacy rights are violated. This could have an impact on the privacy and security policies of Indian internet enterprises. Consumers can not only raise charges of torture, but they can also assert their fundamental right to privacy.

9. CONCLUSION

The term "privacy" has been defined as an individual's right to limit how much of himself he wants to reveal with others. Many states have not explicitly granted individuals the right to privacy, instead relying on legal interpretations. Although the constitutional drafters may not have anticipated the right in question, the technology we have now is significantly different and more advanced than the lives of the generations who drafted the constitution. As a result, the technique of resolution for newly arising problems must be modified, and solutions must undergo a reengineering approach. We hope that the situation for the right to privacy will improve in the future, but the outlook is bleak. Organizations that capture user data have accumulated great influence since the advent of a digital culture with online accounts. While there are certain arguments for collecting user data, there is also a responsibility to manage and secure any personal data that is

collected. Our most valuable possession is our identities. They're a type of riches known as "identity capital." We should expect our personal information to be safe from theft and exploitation.

The United Nations must take the initiative and establish a forum for those whose privacy is in jeopardy. It is the international community's responsibility to promote privacy-enhancing technologies that protect all individuals equally. Online companies must be prohibited from accessing all of our personal information, according to regulations. Users should not be forced to give up their privacy or be denied access to technology they do not want. We must ensure that our personal information is not used without our knowledge or consent, or for reasons that are not clearly declared. Positive steps are being taken, but we are still playing catch-up. The law of privacy was discovered in ancient Indian writings and was available to various areas of protection under the codes. Whatever the case may be, such aspects of privacy protection were not given any thought. Even the Indian researchers did not pay attention. As a result, the 'right to privacy,' as we know it, is most likely a part of present Western legislation. When we examine the current state and trajectory of the right to protection, we find the situation to be unacceptable from all perspectives, including its definition, assurance, scope, confinement, and demand. By coincidence, the privilege that evolved into an element of general law was initially considered a piece of private law. In this way, the desire for security collided with the interests of the broader public.

10. REFERENCES

1. Asher, Jeff and Arthur, Rob. “Inside the Algorithm That Tries to Predict Gun Violence in Chicago”. The New York Times. June 13, 2017: https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagoshigh-risk-list.html

2. Patton, D. U., Brunton, D. W., Dixon, A., Miller, R. J., Leonard, P., and Hackman, R. (2017). Stop and Frisk Online: Theorizing Everyday Racism in Digital Policing in the Use of Social Media for Identification of Criminal Conduct and Associations. Social Media+ Society, 3(3), 2056305117733344: http://journals.sagepub.com/doi/full/10.1177/2056305117733344

3. Human Rights Watch. “China: Police ‘Big Data’ Systems Violate Privacy, Target Dissent” November 19, 2017: https://www.hrw.org/news/2017/11/19/china-police-big-data-systemsviolate-privacy-target-dissent

4. 2016-התשע"ז, האינטרנט] “A bill to remove content whose publication constitutes a crime on the internet, 2016]: http://main.knesset.gov.il/Activity/Legislation/Laws/Pages/LawBill.aspx?t=lawsuggestionssearch h&lawitemid=2011567 תזכיר חוק הסרת תוכן המהווה עבירה מרשת האינטרנט .חוק הפייסבו .Tehila, Eltsholer Schwartz]

5. [2016-התשע"ו] “The Facebook Law. A memorandum on the law for the removal of content that constitutes a crime on the internet]: https://www.idi.org.il/knesset-commities/12069

6. The Israeli Security Agency. “Kalkilya Resident Linked to Hezbollah Arrested and Charged”. March 9, 2017: https://www.shabak.gov.il/english/publications/Pages/296.aspx\

7. Hopkins, Nick. “Revealed: Facebook's internal rulebook on sex, terrorism and violence”. The Guardian. May 21, 2017: https://www.theguardian.com/news/2017/may/21/revealedfacebook-internal-rulebook-sex-terrorism-violence?CMP=share_btn_tw.

8. An Internet Browser interprets HTML the programming language of the Internet, into the words and graphics that are seen my Internet users when viewing a web page.

9. Spam is the use of e-mail addresses for a purpose that consumers have not consented for and constitute a violation of personal rights.

10. "US Report to Congressional Requesters on Medical Records Privacy",www.epic.org/privacy/medical/gaomedical-privacy399.pdf.

11. M. Vijaya v. Singareni Collieries Co. Ltd., AIR 2001 AP 502.

12. http://www.business-standard.com/article/economy-policy/privacy-a-fundamental-right-here-are-5- concerns-with-aadhaar-117071900278_1.html

13. Clause 33(b) of the National Identification Authority of India Bill, 2010.

14. Kharak Singh v.State of Uttar Pradesh, (1964) 1 SCR 332.

15. M.P. Sharma v. Satish Chandra, AIR (1954) SC 300. 68Basheshar Nath v. Commissioner of Income Tax, AIR 1959 SC 149.

Corresponding Author

Dr. Aradhana Parmar*

Dean, Faculty of Law, Maharishi Arvind University, Jaipur-302041 (Rajasthan)