RIGHT TO PRIVACY IN CYBERSPACE

Written by ***Amisha Rerru Singh***

Sharda University, Greater Noida, Uttar Pradesh, India

ABSTRACT

Cyber privacy is a disputed and unsettled issue in legal jurisprudence around the globe. The power of the new slogan, termed 'Information Technology,' has engulfed the present cosmos in the modern era. Individual privacy has risen to the forefront of the Jurisprudential conscience as a result of the sempiternity of knowledge in the midst of the 'Information and Communication Technology Revolution.' Even while the general population lives and transacts as effortlessly online as they do offline, people are not regulated or held by any standards in cyberspace. As more of our regular lifestyle shift online, aided in large part by the ongoing COVID-19 pandemic and quickly evolving technology, we must consider what cyber-protections we have readily accessible and the corresponding standards of protection of our valuable data. It is questionable to what extent residents of democratic countries would be prepared to provide as well as at the same time protect sensitive information. However, it is the legal domain's job to develop an appropriate policy for protecting online privacy from cyber spying, cyberstalking, corporate espionage, devastating cyber-attacks, and website defacement.[1]

As a corollary, the researcher in this research paper tries to find out likely outcomes to assess those things that can be useful for our legislature to get an opportunity to construct a concrete base for setting standards, enacting guidelines, and conducting further research related to the evolving technology era's possible problems and solutions regarding right to privacy. Moreover, this research paper places reliance on the Constitutional Right to Privacy vis-à-vis the arena of cyberspace.

[1] Ed Hagen, Prosecuting Computer Crimes – Department of Justice, OLE Litigation series, (Jan. 21, 2022, 11:06 AM), https://ww.justice.gov/criminal/file/442156/download.

Keywords: Cyberspace, Right to privacy, Individual, Data, Crimes, Information and Technology.

MEANING OF CONSTITUTIONAL RIGHT TO PRIVACY

When somebody comes across its meaning, the concepts privacy and confidentiality are abstract. It has been used in a variety of ways in various situations and circumstances. According to ***Black Law Dictionary***, "the right to privacy" is a "collective term covering multiple rights recognized to be inherent in the concept of ordered liberty, and such rights protect individuals' freedoms to make fundamental choices involving themselves, their families, and their relationships with others."[2]

The legitimate claim of an individual to select the amount to which he desires to share oneself with others, as well as his choice of information about the time, place, and circumstances in which he communicates with others, has been described as privacy in a general sense. It refers to his ability to retreat or participate in any way he thinks fit. It also refers to an individual's right to govern the transmission of personal information since it is his chattel.

Right to privacy, on the other hand, refers to a man's right to be left alone and to be devoid of undesired publicity. The term "right to privacy" is a general term that incorporates a number of rights that are acknowledged as inherent in the concept of organized liberty in the modern era. The right to personal liberty, as well as the ability to travel and speak, all contributes to the right to privacy.

"Privacy postulates the reservation of a private space for the individual, described as the right to be left alone," according to Dr. D.Y. Chandrachud. The individual's autonomy lies at the heart of the concept. The concept of privacy allows an individual to establish and govern the human element that is inextricably linked to their identity. The primary factor in determining the areas of personal importance exemplifies the inviolable quality of the human psyche. Individual autonomy is related with issues that can be kept hidden as well depending on the

[2] Henry Campbell Black, What is PRIVACY? (Definition of Privacy), Black Law Dictionary, (Jan. 21, 2022, 3:33 PM), https://thelawdictionary.org/privacy/.

liberty an individual is subject. These are concerns about which a reasonable expectation of privacy exists.[3]

The mind and body are inextricably linked in the human consciousness. The body's integrity and the mind's sanctity can only exist if each individual has the unalienable ability and right to protect a private space in which the human individuality can grow. The personality's inviolability would be questioned if it lacked judgment in making a trait.[4]

Acknowledging a personal space is just acknowledging that each person has the right to plan and explore their own path of personality development. As a result, privacy is a tenet of human dignity. Thoughts and behavioural patterns that are personal to an individual are privileged to a private space devoid of social pressures. A human is not assessed by others in that sphere of solitude. Individual privacy allows each person to make important decisions that are reflected in their personality. It allows people to hold on to own views, thoughts, expressions, ideas, philosophies, preferences, and choices in the face of societal homogeneity expectations.[5]

"Privacy is an inherent affirmation of variance, of the individual's right to be distinct and to create a solitary zone in defiance of the tide of similarity. Privacy shields a person from the prying eyes of the public in concepts that are personal to him or her. Privacy pertains to the individual rather than the location with which they are affiliated. Because the person can select how liberty is best enjoyed in privacy, privacy is the cornerstone of all liberty. Individual dignity and privacy are closely interwoven in a pattern of the fabric comprising of a multiple civilization forming a thread of diversity."[6]

Right to Privacy in the Realm of Cyberspace and its Significance

The current world order specifies two kinds of privacy. The first is privacy in the real life, which can be defined as minimized level of intrusion into one's physical space or solitude; the second is privacy in the virtual environment, also known as cyber space, which refers to the collecting of user information from a multitude of sources, including the internet. Information

[3] Justice K.S. Puttaswamy (Retd.) and Anr. vs. Union of India & Ors., (2017) 10 SCC 1.
[4] *Id.*
[5] Nidhi Singh, Justice K.S. Puttaswamy (Retd.) and Anr. vs. Union of India, NLU Delhi, (Jan. 23, 2022, 4:17 PM, https://nludelhi.ac.in/library-dig-data.aspx.
[6] *Id.*

collecting, processing, publication, and breach of private data are all examples of privacy and its corresponding aspects in the virtual world.[7]

People appear to be more immersed in the digital world, also known as cyber world, as a result of rapid technology breakthroughs and rising internet use. Platforms like Facebook and Twitter are helping to facilitate this addiction to a greater level. Websites like Facebook, Twitter, Instagram, and YouTube have nearly two billion active users and offer applications and features including communication, photo and video posting, and sharing.[8] These websites collect, store, and process a large amount of personal information on their databases, which are frequently located outside of India's territorial jurisdiction. Theft or security breaches of this data by a third party pose a little and sometimes a wide-ranging risk to an Indian subscriber of these websites.

The Information Technology Act, which was particularly intended to offer legal status to e-commerce in India, is vague on these corporations' liability with regards to third-party use of this data without the user's consent. The act makes no use of the phrase "cybercrime." Some scholars refer to this Act as "toothless law" because of its ineffectiveness in enforcing punishments or repercussions against those who chose to abuse cyberspace's coverage. As a result, there is a legal vacuum that must be filled as soon as possible.

Digital Footprint

Every netizen leaves a digital footprint (a digital trace of data created by a person while using the internet.) This comprises web pages visited, emails exchanged, and information supplied online. When someone uses the internet, certain information is compiled at times, even without the person's knowledge. As a result, digital footprints can be grouped into two categories i.e. Active and Passive digital footprint.[9]

When we talk about active digital footprint it comprises of publically identifiable data that you communicate on the web, such as data submitted on Facebook, Instagram, or other social

[7] Steve Symanovich, Privacy vs. Security: What's the difference – Norton, Nortonlifelock, (Jan. 24, 2022, 10:22 PM), https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html.
[8] `Most Used Social Media 2021| Statista, Statistical Research Department; Europe, (Jan. 25, 2022, 6:09 PM), https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.
[9] Kristina Ericksen, What is your digital footprint | IT PRO, (Jan. 26, 2022, 4:15 PM), https://www.itpro.co.uk/strategy/29259/what-is-your-digital-footprint.

platforms, as well as any other information that the individual keeps posting for personal activity. The data that a private corporation accumulates behind the curtains or veils of technology, such as IP address, transaction information, navigation details, and location so on, is known as a passive digital footprint.[10]

This digital footprint, along with many other users' data, is now recurrently used by companies alone without user's prior consent to identify and detect habits of a user's behaviour; however, this data is also used by a private person to commit illegitimate or immoral acts, such as morphing, which was the most common cybercrime against women just few years ago, in which publicly available photographs of females were transformed to offensive pictures thereby breaching privacy.

The Facebook-Cambridge analytica scandal, which involved the collection of 50 million of the subscribers' Facebook profile data through the use of a third-party application called "this is your digital life," which tempered with Facebook login, was the worst data exploitation event of all period in 2017. Cambridge analytica used this information to try to sway public sentiments of various political organizations.[11]

Technological has a nasty aspect since it makes commercial activities easier. Normally, the law keeps up with technological advancements, but the rate of technological advancements in recent years, particularly in the sphere of information and technology, has made it impossible for the legal system to stay up. Modernizing penal laws in many nations that predate the invention of computers is a major concern. On the one hand, current laws must be changed to address device criminality such as hacking, deliberate fabrication or elimination of data, technology theft, software threats, and so on; on the other hand, new legislation is required to safeguard data security and piracy.

LAWS GOVERNING DATA PRIVACY TILL DATE

[10] *Id.*

[11] Jason McElweenie, The Fallout from Facebook's Cambridge Analytica data crisis, Daily Dot, US, (Jan. 26, 2022, 7:09 PM), https://www.dailydot.com/debug/facebook-cambridge-analytica-timeline/.

There is currently no explicit legislation in India addressing data protection or privacy. The Information Technology Act, 2000 and the Contract Act, 1872 are the important data protection statutes in India presently. In India, a standardized data protection law is expected to be enacted in the coming years. The Information Technology Act, 2000 investigates complaints relating to civil compensation and criminal penalties for improper revelation and exploitation of personal data, as well as breaches of contractual agreements pertaining to personal data.

A body corporate that is in possession, dealing, or handling any sensitive personal data or information, and is negligent in implementing and maintaining reasonable security practices, resulting in wrongful loss or wrongful gain to any person, may be held liable to pay damages to the person so affected under *section 43A of the Information Technology Act, 2000*.[12] It is crucial to highlight that the reimbursement that can then be requested by the harmed party in such instances has no maximum limit fixed under the statute but governed by the rule of damages under the Contract Act.[13]

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, have indeed been enacted further to strengthen the regime of data privacy. The Guidelines only cover the safeguarding of "vulnerable private and confidential information/data of a person," which includes a range of comprehensive definitions such as:

"Password, financial information (such as bank account/credit card/debit card/other payment instrument) details, Physical, physiological and mental health conditions, Sexual orientation, Medical records and history, Biometric information."[14]

According to *section 72A* of the IT Act, 2000, which states that if a person knowingly and intentionally disclosing information without the consent of the person concerned and in violation of a legitimate contract is punished up to three years imprisonment and a fine of up to Rs 5,00,000.[15]

[12] Information and Technology Act, 2000 (No.21 of 2000), Section 43A.
[13] *Id.*
[14] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, (Department of Information Technology, Government of India), Rule 2.
[15] Information and Technology Act, 2000 (No.21 of 2000), Section 72A.

It should be acknowledged that *section 69* of the Act, which is an exception rather than the basic policy/rule of maintaining private data and secrecy, provides that where the Government is satisfied that it is essential as to the function of India's sovereignty, defensive tactics, safety, cordial relations with foreign entities, or public order, or for blocking incitement to the commission of any cognizable offence pertaining to the above, or for any investigative purposes, the Government may disclose details as and when required.[16]

However, in the 52nd Report on Cyber Security and Right to Privacy, the Parliamentary Standing Committee on Information Technology stated that an extreme rise in cyberspace activities and access to the connectivity in India, coupled with a lack of user end discipline, inadequate computer system protection, and the possibility of unidentified use of ICT allowing users to impersonate and cover their criminal trends, has empowered more users to experiment with ICT abuse for nefarious purposes.[17] This component, according to the Committee, has a substantial impact on neutralizing the deterrent effect established by the legal structure, which is not aptly recognized by the IT Act, 2000 and related statutes.[18]

The statute was amended in 2008, particularly known as the Information Technology Amendment Act, 2008 which incorporated several safeguards to protect a person's privacy from internet intrusion and exploitation. It includes fines and prison sentences for hacking (Sections 43, 66), three years in prison for privacy violations (Section 66E), identity theft (Section 66 C), and cheating by impersonation (Section 66 D), and abusive email (Section 66 E); (Section 66A).[19]

Unauthorized disclosure of personal information by someone who obtained it through a legitimate contract and without the consent of the person to whom it belonged or was stolen is punishable under Section 72A of the IT Act. A well sorted example of the same is GDPR which was successfully formed by the European Council (EU) in 2018 and is among the most rigorous

[16] Information and Technology Act, 2000 (No.21 of 2000), Section 69.
[17] Elonnai Hickok, CIS Welcomes 52nd Report on Cyber Crime, Cyber Security and Right to Privacy, CIS India, (Jan. 28, 2022, 3:22 PM), https://cis-india.org/internet-governance/blog/cis-welcomes-fifty-second-report-on-cyber-crime-cyber-security-right-to-privacy.
[18] *Id.*
[19] The Information Technology Act, 2008, Ministry of Law, Justice and Company's Affairs, (Legislative Department), (Jan. 29, 2022, 6:18 PM), https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf.

laws to protect the personal data of European Union citizens. This policy has proven to be a significant step forward in the realm of privacy shield. The introduction of this policy has had a significant influence on different tech corporations such as Google, Facebook, and many other prominent e-commerce sites. This rule has undoubtedly established new jurisprudence in the field of cyber law.[20]

Case Laws

In the case of ***Amar Singh v. Union of India,***[21] the Supreme Court addressed the right to privacy in the context of phone call monitoring and recognized the same as an integral part of individual's privacy. Similarly, in the ***People's Union case,*** the question of whether surveillance of telephonic messages/tapping of telephonic conversations constituted a significant infringement of an individual's right to privacy was reviewed in detail by the Hon'ble Apex Court, which decided as follows:[22]

"17. We have no problem in holding that the right to privacy is established in Article 21 of the Constitution as part of the right to "life" and "personal liberty." When the facts of a case give rise to a right to privacy, Article 21 is invoked. The said right cannot be restricted "unless in accordance with legal procedures."[23]

"18. 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"."[24]

Telephonic conversations are frequently personal and private. Thus, telephone is an integral component of contemporary man's life. It is regarded as so vital that an increasing number of people keep mobile telephone equipment in their wallets. A man's private life revolves around his telephonic conversations. These telephone conversations in the privacy of one's house or

[20] EU-US Privacy Shield, Data Protection | European Commission, European Commission, (Jan. 31, 2022, 5:19 PM), https://ec.europa.eu/info/law/law-topic/data-protection_en.
[21] Amar Singh vs. Union of India, (2011) 7 SCC 69.
[22] People's Union for Civil Liberties vs. Union of India & Ors., AIR 1997 SC 568.
[23] *Id*, para 17.
[24] *Id*, para 18.

apartment are unquestionably protected by the right to privacy. Eavesdropping, then, on such conversations would be a violation of Article 21 of the Indian Constitution unless otherwise approved by law.

Furthermore, in the case of ***Vinit Kumar vs. Central Bureau of Investigations and Ors,*** the Bombay High court upheld, *"the constitutionality of breach of confidentiality with reference to small and minute details like wiring, equipments and the requirement of taping phone calls for surveillance purpose only for occurrences that fall under the umbrella of public emergency or the interest of national security."*[25]

In ***Indian Hotel and Restaurant Association (AHAR) v. The State of Maharashtra,*** the Supreme Court regarded that the data kept in CCTV footage to be a person's private information, citing Puttaswamy's decision in support. *"Comprehensive surveillance of actions inside the territory of dance bars by CCTV cameras is excessive and disproportionate, the court said. Monitoring, storing, and retaining dance performances are an unjustified breach of privacy that could possibly put women bar dancers in danger. Because CCTV footage is a reliable source for identifying a person that becomes part of his personal information, triggering his right to privacy."*[26]

Innovation and Technology now has the potential to increase massive data sets that may have been statistically analyzed to show patterns, tendencies, and relationships, particularly in the context of human behavior and interactions around the world. According to the council on Free and Fair Digital Economy's report, *"Data gathering procedures are frequently opaque, bogged in complex privacy forms that are unintelligible, thereby leading to practices that users have little influence over."*[27]

CURRENT LEGAL DEVELOPMENTS UNDER DATA PRIVACY LAWS IN INDIA

[25] Vineet Kumar vs. Central Bureau of Investigation and Ors, Writ Petition (Cri.), 2367/2019.
[26] Indian Hotels and Restaurant Association vs. State of Maharashtra, 2019 (3) SCC 429.
[27] PRS Legislative Research, A free and fair Digital Economy, Committee Reports, PRS India, (Feb. 1, 2022, 10:00 PM), https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy.

The Ministry of Electronics and Information launched the PDP Bill in the Indian Parliament on December 11, 2019, and it is primarily based upon the GDPR Model currently put into operation in the European Union.[28] On November 22, 2021, a joint parliamentary committee reviewed and endorsed a modified application of the PDP Bill.[29] The privacy information by the Govt., enterprises, and global firms will be governed by this prospective statute.

Personal data can be described as *"...data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute, or other feature of such natural person's identity, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling..."*.[30]

The construction of a Data Protection Authority (DPA), comparable to that of the European Union, including the segmentation of personal data which also need to be protected, is one of the far more interesting advances proposed under the PDP Bill. The PDP Bill, for example, uses a three-tiered framework to guarantee data security and localization. Personal data is exempt from data transmission limitations; nevertheless, "sensitive personal data" and "important personal data" are subject to restriction as stated by the central government.[31]

Quantitative statements, personally identifiable information, caste, religion or political convictions, or any other genre of data determined by the Indian government, in collaboration with the DPA and the appropriate sector-specific regulator, is considered sensitive personal data in consonance with the PDP Bill. Furthermore, "essential personal data" is not allowed to be sent outside of India in any circumstance except as those necessitated by the government. Data transmissions to countries or organizations which are priorly judged so as to provide an assurance of safety are permitted to a limited degree.[32]

[28] PRS Legislative Research, The Personal Data Personal Bill, 2019, PRS India, (Feb. 2, 2022, 7:09 PM), https://prsindia.org/billtrack/the-personal-data-protection-bill-2019.
[29] *Id*, pg 1.
[30] Personal Data Protection Bill, 2019, (Ministry of Electronics and Information Technology), Section 3(28).
[31] Arun Sharma, Personal Data Protection Bill can seed uncertainity for businesses, The Economic Times | Rise, (Feb. 2, 2022, 4:19 PM), https://m.economictimes.com/small-biz/policy-trends/personal-data-protection-bill-can-seed-uncertainty-for-businesses-reduce-competitiveness/articleshow/88116148.cms.
[32] Suneeth Katarki, Namita Vishwanath, Ivana Chatterjee, Rithika Reddy Varanasi, India: The Personal Data Protection Bill, 2019 – Mondaq, Mondaq, (Feb. 3, 2022, 8:09 PM), https://www.mondaq.com/india/privacy-protection/880200/the-personal-data-protection-bill-2019-key-changes-and-analysis.

In contrast, the PDP Bill mandates a series of criteria on data controllers (including social networking middlemen) in terms of how they receive, manage with/process, and keep personal data. It holds them responsible for abiding to the requirements of a complete series to the transfer of personal information carried out by it or on its account.[33] Data fiduciaries, for example, are responsible for putting in place methods for age verification and parental authorization whenever managing highly sensitive data concerning children.

In addition, processing or transferring data in defiance of the PDP Bill carries harsh penalties. An infringement under the PDP Bill seems to have a maximum pecuniary penalty of INR 15 crore.[34] The DPA also makes processing of de-identified private information without approval illegal by up to three years imprisonment, and fine, or both. The PDP Bill proposes to create an appellate body to hear first-round appeals against the DPA's judgment, with a second-round appeal presented to the Supreme Court of India.[35]

CONCLUSION

A person's existence has now significantly grown in the electronic dimension known as the cyber world as a result of changing times urging for a need to switch to the virtual world on one hand and heavy emphasis on technology and the internet on the other. This exposure has the potential to endanger a person’s physical life and obstruct fulfillment of his rights. An Individuals’ virtual privacy must be recognized and protected as soon as possible to protect them from large scale harm. The European Union’s General Data Protection Regulations contain rigorous and systematic rules and will serve as a model for future data protection legislation in India.[36]

The Personal Data Protection Bill has a multitude of conformity procedures in it, so it could be a good place to start when it comes to regulating corporations that hold user data in India. In addition, the Act establishes a penalty structure to function as a disincentive where non-compliance occurs. Economic and commercial interests, as well as the authenticity of a person's

[33] *Supra* note 31.
[34] Supratim Chakraborty, India: Data Protection Laws and Regulations 2021, ICLG India, (Feb.4, 2022, 4:28 PM), https://iclg.com/practice-areas/data-protection-laws-and-regulations/india.
[35] *Supra* note 32.
[36] *Supra* note 20.

virtual existence, should be considered while assessing these compliance and sanctions. Other nations' legislations on the other hand inculcate the mechanism, particularly on the subject of cross-border data transfers, and the same should be examined in order to make the law more consistent and interoperable.

Yet there is a good argument to be made in justification of the PDP Bill, it can also be asserted that the Government of India has evolved from inadequate monitoring of cyber and data security in India to developing an effective system for the same. Many adversaries have voiced doubts about the Indian government's overstepping powers under the PDP Bill, such as the ability to legislate what qualifies essential personal data, and furthermore many international firms believe the planned reforms are too stringent to comply with. Although the Indian government is inclined to adopt the bipartisan parliamentary committee's proposal of the PDP Bill, whereby a number of key concerns about data security in India are required to be addressed.

Not just for the common Indian person, but also for the sovereignty of the nation, the enforcement tactics stated above are vital. Given the foregoing, it is reasonable to conclude that, whilst the IT Act and its additional policies, rules, and norms have evolved and progressed since their establishment, they are insufficient to ensure data security and safeguard against cyber dangers.