Privacy Regime In Cyberspace – Indian Quest For Privacy And Data Protection Left Under The Shadow Of An Evolving Virtual World

By Elizabeth, B.com LLB(Hons) at His Highness Maharajas Govt. Law College

INTRODUCTION

Cyberspace is a rapidly growing network of communication that has been deeply rooted in our society. Any activity from shopping, medicines, consultations, transactions, e-filing, e- rentals etc. are available at our doorsteps at a single click on the internet. However, despite all these benefits, cyberspace has put forth a great concern in the modern world – "the interference on the right to privacy". As we know privacy is one of the cornerstones of a democratic society, it needs to be protected in the cyber world just like the physical world.

Intermediaries act as road providers in this virtual space. As if we go to a physical market anything and everything is available in the internet market. Anonymity and secrecy being the core benefits of this market, the trend shows a great inclination of people towards online products and services. On the other hand, every activity in the virtual space is closely spied on, observed and noted by an invisible rapporteur. All the data generated on the internet are detailed, computer-processed, indexed to each individual and permanently stored. These data have great potential to reveal our identity.

The concept of privacy preaches that in every public sphere there is a private sphere that should be left without intrusion and intervention, freely enjoyable by the individual. Privacy has a deep role to play in today's life. Nevertheless, surveillance in the private sphere has increased largely with the advent of cyberspace. Cybercrimes like data theft, identity theft, hacking, spoofing, spamming, cyber-stalking, cracking, page jacking etc. are the new menaces that society needs to combat. On this road, the Judiciary has taken a pragmatic step towards recognizing and protecting privacy in the cyber regime. In the absence of compact legislation, India is far behind other countries in the arena of data protection.

PRIVACY - EVOLUTION OF THE CONCEPT

"The right to privacy is a sacrosanct as human existence and is inalienable to human dignity and autonomy". – Dr D Y Chandrachud, J[1]

Privacy is a cluster of rights that extend from the right to have a private sphere to the right to decide on what personal information of oneself should be released in the public sphere, its quantity and quality. Privacy is a complex idea that determines an individual's ability to take a certain decision without interference, the extent to which an individual's territorial solitude is protected from invasion and the control on the acquisition, use, flow and disclosure of information. Privacy has both positive and negative perspectives. The positive aspect reflects one's right to self-development and its negative connotation reflects a person's right to be let alone. It determines one's autonomy over personal information and identity. All information about a person is their asset that they fully retain and use. The core of information privacy is thus a right to autonomy and self-determination in respect of one's data.

The jurisprudence of the Right to Privacy has evolved through various judicial interpretations in India. From a no privacy regime to an implicit right period and finally to an explicit fundamental right under the constitution through the *2017* Puttaswamy case, the changing phase of privacy witnessed great challenges.

MP Sharma v. Satish Chandra[2] was the first occasion where the Supreme Court attempted to mark the perimeter of privacy under the Indian Context. Here the validity of search and seizure by police authority was challenged as against right to property under Article 19 (1) (f) and right against self-incrimination under Article 20(3). The concept of privacy was new for the Court and it took a stagnant step by holding privacy to not be a fundamental right. Further, this aspect was again brought up before the Supreme Court in the case of Kharak Singh v. State of Uttar Pradesh[3], which dealt with state surveillance against the right to privacy. Here again, the court reiterated that "the right of privacy is not a guaranteed right under our Constitution and, therefore, the attempt to ascertain the movements of an individual which is merely a manner in which privacy is invaded is not an infringement of a fundamental right guaranteed by Part III."[4]

---

[1] Justice K. S. Puttaswamy and ors v. Union of India, (2017) 10 SCC 1.
[2] M P Sharma v. Satish Chandra, District Magistrate, Delhi (1954) SCR 1077 M P Sharma v. Satish Chandra, District Magistrate, Delhi (1954) SCR 1077
[3] Kharak Singh v. State of Uttar Pradesh (1964) 1 SCR 332
[4] Id 3

In Malkani v. State of Maharashtra,[5] the admissibility of tape-recorded messages was challenged in line with privacy norms before the Supreme Court. The petitioner contended that the tape-recorded evidence was inadmissible, as it was not procured through a procedure established by law. The court relied on the observation made in R. v. Leatham[6] that "It matters not how you get it if you steal it even, it would be admissible in evidence". The Apex Court took the same road and held that "As long as it is not tainted by an inadmissible confession of guilt, evidence even if it is illegally obtained is admissible."[7] In Amar Singh v. Union of India,[8] The Supreme Court took a similar view by observing that interception of phone calls is an invasion of the right to privacy under the Constitution.

In the State of Maharashtra and Ors. v. Madhukar Narayan,[9] The Apex Court elevated the status of privacy by observing that, "Even a woman of easy virtue is entitled to privacy and no one can invade her privacy as and when he likes. She is entitled to protect her person if there is an attempt to violate it against her wish. She is equally entitled to the protection of the law."[10]

Ramlila Maidan v. Home Secretary, Union of India[11], Gobind v State of Madhya Pradesh[12] and Mr X v. Hospital Y[13] are some other landmark decisions that instilled the pillars of privacy in India. Privacy as an essential ingredient of life and liberty was widened through these judicial interpretations. Though privacy was an implicit and alien concept during the inception of our constitution, it gained much attention through a tiresome judicial procedure. Law is never static and it evolves with the needs of society.

Privacy occupied an epitome position through the interpretation of the Supreme Court in Justice K. S. Puttaswamy and Ors. v. Union of India.[14] The validity of the Aadhaar Act 2016 was challenged as a violation of the right to privacy in this case. The Apex Court took a pragmatic approach by declaring the right to privacy as part and parcel of the Right to life and liberty under Article 21 of the Constitution. The Court held that "Privacy is the constitutional core of human dignity. Privacy has both a normative and descriptive function. At a normative level,

[5] Malkani v. State of Maharashtra, 1973 AIR 157, 1973 SCR (2) 417
[6] R. v. Leatham, (1861). 8 Cox CC 498 at 501
[7] Id 4
[8] Amar Singh v. Union of India, (2011) 7 SCC 69.
[9] State Of Maharashtra and Another vs Madhukar Narayan Mardikar, AIR 1991 SC 207, 1991 (61) FLR 688
[10] Id 7
[11] In Re Ramlila Maidan Incident, (2012) 5 SCC 1
[12] Gobind vs State of Madhya Pradesh And Anr, (1975) 2 SCC 148, 1975 3 SCR 946
[13] Mr X v. Hospital Y, 1998 Supp (1) SCR 723
[14] Justice K. S. Puttaswamy and ors v. Union of India, (2017) 10 SCC 1.

privacy sub serves those eternal values upon which the guarantees of life, liberty and freedom are founded. At a descriptive level, privacy postulates a bundle of entitlements and interest which lie at the foundation of ordered liberty."[15] The very recent Pegasus spyware attack case[16] also reiterates the essence of privacy in practice. Thus, privacy is no longer an alien concept in our system but a judicially moulded concept that pillar the core values of our constitution.

PRIVACY LAWS IN INDIA

India does not have comprehensive legislation on privacy protection. The right to privacy is enshrined under Article 21 of the constitution, which can be enforced through constitutional remedy under Article 32 and Article 226. Any intrusion on privacy must be by a procedure established by law and should pass the test of reasonableness and proportionality. The Information Technology Act 2000 and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("Data Protection Rules") are the mother legislation on data protection in cyberspace. The provisions of the Indian Penal Code 1860, Contract Act 1872, Copyright Act 1957, Consumer Protection Act 2019, and the Indian Telegraph Act 1885 also provide a vague framework on information protection.

After the landmark Puttaswamy judgement, a committee was formed, led by retired Supreme Court judge B.N. Srikrishna, to devise a draft law on data protection. The Personal Data Protection Bill, 2019 was put forth before the assembly as a culmination of preserving privacy in the changing cyber era. However, the law is still on wheels – a long way to go from paper to practice.

CYBERSPACE AND DATA PROTECTION

Protection of personal data holds the key to empowerment, progress, evolution and innovation. With the advent of cyberspace, the world has shrieked to a monitor and through a single click one can reach out to every corner of the globe. Regardless of its merits, the virtual world is the arena of the majority of offences in the modern world.

[15] Id 13
[16] Manohar lal Sharma v. Union of India and ors., writ petition (crl.) no. 314 of 2021

Many of the applications we use today have permission columns at the stage of installation. We often ignore such terms and conditions and consent to every term without even having a good read. Each transaction we make on the internet, each search in the search engine and even search entry to websites leave behind their footmarks, easily accessible by the market players. This opens up a gate for the intruders to thrive on the data of the host. The very technology that made us invisible can thus identify our identity by following the footprints in the virtual world. Many of these data are being sold and prioritized by intermediaries or hackers. Any unauthorized access to personal information and activity or manipulation or misuse of this information affects the privacy of an individual seriously. To worsen the matter, often these unauthorized usages may not come to one's notice until it is too late to heal the injury.

The IT Act, 2000, along with the IT rules of 2011, is the mother legislation protecting data and securing information privacy in India. Section 72 of the IT Act provides for penalties on data breach and confidentiality/ privacy intrusions. However, the scope of the Act is limited in the growing cyber regime. The majority of the provisions only apply to sensitive personal data and its reins are often extended only to corporate entities[17]. Sensitive data under the 2011 rules include an exhaustive list of entries from passwords, financial information, account details, sexual orientation, medical history and records, biometric information[18] to any other information stored and processed by body corporates.[19] Thus, the law has left behind a vacuum that excludes any private party engaged in non-commercial activities and using sensitive information outside the purview of penalty. This lacuna is exploited by the crooked cyber market players to safely harvest information escaping the law of the land. Further, only those sensitive personal data or information that are in electronic form or stored in a computer device are construed under the ambit of the IT Act. The rules also prescribe the body corporates to take consent of the parties concerned before collection, storage and dissemination of such sensitive information,[20] but the law is silent on the scope of retrieving the consent and right to erase the data once shared.[21]

[17] Section 43 A of Information Technology Act, 2000
[18] Sub-Rule (vii) of Rule 3 of the 2011 Rules
[19] Sub-Rule (viii) of Rule 3 of the 2011 Rules
[20] Rule 5(1) , 5(2), 5(3), 5(4), 5(5), 5(6)of the 2011 Rules.
[21] Vinod Joseph , Protiti Basu and Ashwarya Bhargava, India: A Review Of The Information Technology Rules, 2011 Reasonable Security Practices And Procedures And Sensitive Personal Data Or Info, Mondaq, 19 March 2020, Available at: https://www.mondaq.com/india/privacy-protection/904916/a-review-of-the-information-technology-rules-2011-

Cyberspace has no territorial limits; it is spread globally and transactions take place without the barrier of the medium. Determining the jurisdiction of cyber activities is very vital to take action against any illegal activity. However, jurisdictional limits pose a challenge to data protection.

As observed by the Supreme Court in the Puttaswamy case, "Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State". Law attempts to balance the right to privacy of an individual and the security interest of the state but it cannot simply trade-off one for another. Building privacy values into cyber security policy direction is the need of the hour to create a secure cyber regime.

THE LEGAL LACUNAE

The greatest challenge faced by India in the global cyber sphere is the lack of comprehensive legislation to address all the cybercrimes and frauds happening around in the virtual world. Though a bill was introduced in the Parliament in this regard, it has not been passed yet. The existing legal framework is inadequate to curb the cyber-attacks on individual rights. Further, there is no definite classification of information into private and public to determine the strengthened protection required. It is also evident that the technological infrastructure to store, process and disseminate data is weak and inadequate to handle cyber threats. The lack of guidelines for the cross-country flow of information further deteriorates the situation. India has emerged as a global market for online activities, which has also made it prone to a variety of cyber-crimes varying from identity theft, scamming, fraud, data theft, piracy, pornography, cyberstalking, cheating and many others. There is an immediate need for a regulatory mechanism to closely observe cyber activities across the country. The complex interlinked environment and evolution of cyberspace further challenge privacy and security. The intermediaries also take advantage of the safe harbour exemption provided in the IT Act to clean their hands from any illegal activity. This legal lacuna needs to be gapped to provide a secure cyber experience in India.

CLOAK AND DAGGER SURVEILLANCE OF THE STATE IN CYBERSPACE– A THREAT TO PRIVACY

Under Section 69 of the Information Technology Act, 2000 the Central Government is empowered to impose reasonable restrictions on rights of individuals in cyberspace, intercept, decrypt or monitor Internet traffic and data on grounds of national security, integrity, friendly relations with other countries, public order and decency or to prevent incitement of any offence. However, on various occasions, this power was misused by the Government to threaten the privacy of an individual. There was a huge public outcry questioning the validity of IT (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 that permitted the home Secretary in the Home Ministry to authorize agencies to decrypt or monitor the internet activities of the suspects.

Such surveillance is an inevitable compound in today's cyber era but the scope and extent of such powers need to be tested against the ground tests involved in our country. Any diversion from ethical and legal stand would be a planned invasion of privacy and state surveillance.[22]

The recent Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 has raised great concern from the public as it is believed to be a disguised attempt of the government to intrude on the privacy of individuals o the face of national interest.[23]It is considered as a precursor of anti-encryption legislation to evade private rights. The new rule prescribes due diligence to be taken by the Social Media Intermediaries in cyberspace to detect cybercrime in cyberspace and speedy mechanism to put down any illicit content from the media and to incorporate grievance officers to provide speedy remedy to the victim. The controversy pertains to the obligation of the intermediary to identify the first originator of the information. Thus, it is a direct hit on the anonymity of the user and denies his privacy. In the paper, it appears to be an empowering provision to curb cyber-crimes plaguing the virtual world but in practice, this provision has the potential to be politicised and used as indirect censorship on social media content. In the current scenario where the law is

[22] Tathagata Satpathy, Karnika Seth, Anita Gurumurthy, Are India's Laws on surveillance a threat to privacy, The Hindu, 28 December 2018, Available at: https://www.thehindu.com/opinion/op-ed/are-indias-laws-on-surveillance-a-threat-to-privacy/article25844250.ece

[23] Raghav Tankha, The Information Technology Rules 2021: An assault on Privacy as we know it, Bar and Bench, 09 Mar, 2021, Available at: https://www.barandbench.com/columns/the-information-technology-rules-2021-an-assault-on-privacy-as-we-know-it

used as an instrument to oppress dissent, the new rules will further support the existing draconian laws in our country. Just like UAPA in the physical world, the IT Act cannot be moulded and has been equipped as a weapon to dilute privacy and liberty.

The recent case of the Pegasus spyware attack itself shows the loopholes in our cyber system and states should take full responsibility and accountability to safeguard personal rights balanced with the national interest. Any law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. The procedure should be just, fair and reasonable. It should also meet the threefold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them.[24]

CONCLUSION

We live in an age of information revolution. Data has utmost value in this system and therefore the illegal means of acquiring and disseminating information is a menace that plagues the cyber world. The connotation of life under Article 21 of the constitution narrates that life is not just an animal existence but it includes the right to live with dignity and liberty. Privacy is an aspect of life and it cannot be invaded in any sphere. Privacy has both positive and negative implications. The negative content restrains the state from infringing the life, liberty and privacy of a citizen. Its positive content imposes a duty on the state to take all necessary measures to protect the privacy of an individual.

Many of the offences take place because of the negligence of internet users. Passwords are weak or being shared, not logged out of the system, agreeing to policy agreements without having a closer look into the clauses, using pirated soft wares, not installing a proper virus guard and many others. Therefore, what is required is to give proper technological education and awareness among people on the use of cyberspace and its grey sides. Breach preparedness is still not taken up as a priority. People must be more cautious about permitting access to sensitive information and data. In India, we still have a consent-based approach that undermines the right of the customer once the data is shared to body corporates. There is an immediate need to shift the consent approach to a rights-based approach that provides

[24] Id 16

autonomy to the data holder. Many of the websites that once collect the data do not delete them later, the right to be forgotten is equally applicable in the cyber world that needs to be emphasised. Explicit consent practice should be followed by intermediaries handling sensitive data and personal information.

The greatest challenge in the Indian cyber economy is the absence of umbrella legislation to secure data. The data protection bill is the only hope for a bright future. A Data protection authority should be established to provide grass root level grievance redressal. Also, there should be Data localisation that encourages local companies to take in the task of data protection. In the current setup, international corporations are the active market players in data processing and protection. However, a shift in this trend would make our country self-sufficient in data handling. Technological capacity building, infrastructural development and investment in data security technology should be encouraged. An integrated stewardship approach of all the stakeholders- the users, intermediaries, corporates, government, government agencies can only pave the path to a secure cyber environment. A proper balance of citizens' privacy and the state's interest is the need of the hour.