

## THE RIGHT TO PRIVACY IN THE DIGITAL AGE

Mr Sanjay Kumar Pandey\*

“At its best, the digital revolution will empower, connect, inform and save lives. At its worst, it will disempower, disconnect, misinform and cost lives.”

**-Michelle Bachelet, UN High Commissioner for Human Rights**

### ***Abstract***

*Privacy is the right to be free from unwarranted intrusion and to keep certain matters from public view. As such, “Privacy is an important element in the autonomy of the individual. Much of what makes us human comes from our interactions with others within a private sphere where we assume no one is observing. Privacy thus relates to what we say, what we do, and perhaps even what we feel”.*

*Digital technologies do not exist in a vacuum. They can be a powerful tool for advancing human progress and contribute greatly to the promotion and protection of Human Rights.*

*However, data-intensive technologies, such as artificial intelligence applications, contribute to creating a digital environment in which both States and business enterprises are increasingly able to track, analyze, predict and even manipulate people’s behavior to an unprecedented degree. These technological developments carry very significant risks for human dignity, autonomy and Privacy and the exercise of Human Rights in general, if applied without effective safeguards.*

*Whether the threat comes from governments or private entities, these occurrences pose a significant question as to the Right to Live without arbitrary attacks on Privacy (Article 12 of the Universal Declaration on Human Rights) and how our right to safeguard privacy can be defended.*

---

\* Asst. Professor @ Amity Law School, Amity University Haryana, Gurugram

## INTRODUCTION

Digital technology has transformed the means through which Human Rights are both exercised and violated around the globe. The Internet has become an indispensable tool for the realization of a range of Human Rights, and for accelerating economic development. Yet, every day, there are new examples of how digital technologies play a role in undermining Human Rights whether through a Prime Minister banning Twitter in Turkey; a death sentence for a posing on Facebook in Iran; bulk electronic surveillance of American citizens by the NSA; a Court ruling on the right to be forgotten in Google searches in Europe; or a requirement that Internet users supply real names to service providers in China. This dual edge aspect of technology was conveyed well by a Tibetan Human Rights activist to the Toronto-based research group Citizen Lab: “Technology is this funny thing where it’s a lifeline, and then . . . maybe it’s your ticket to jail.”

The need of the hour is to find solutions which can ensure that the Right to Privacy is protected and its infringement is duly sanctioned.

Firstly, privacy being a global concern, the international governance has to play an effective role in defining the term privacy which has universal applicability. This will ensure stability regarding the purview of the term privacy in a way that all the parties are able to enforce this right in case of violation at the national and international platform as well.

Secondly, as it was being stated at the RSA Conference that the need is to utilise the knowledge and skills of content managers, architect and IT engineers to prevent digital attacks with the sufficient and effective preventive steps. Therefore, the IT developers must invent innovative and new ways to prevent cyber-attacks.

Thirdly the requirement is to increase the involvement of civil society by making them aware about the ways to ensure protection of personal data in this digital world. There should be encouragement from various political activist and NGOs on the public to prevent the violation of their Right to Privacy. For instance the civil society organizations and various experts from all over the globe have established 13 International Principles on the Application of Human Right to Communication surveillance”. On the basis of these principles they are requesting the respective governments to conduct communication surveillance that shall be consistent to Human rights.

## **SURVEILLANCE: A THREAT TO DEMOCRATIC SOCIETY**

The Apex Court, on 27 October 2021, ordered for the formation of an independent expert committee to investigate the allegations related to surveillance of politicians, activists, journalists, and constitutional authorities, using the Pegasus Spyware. The Committee will be headed by Justice RV Raveendra, former Supreme Court Judge.

Pegasus Spyware is developed by the Israeli cyber firm NSO. It has targeted hundreds of phones in India. The Spyware can enter the device of the targeted of phones in India; the spyware can enter the device of the targeted person without even their knowledge, because it is designed in such way that it can impersonate itself a downloaded application in the phone and transmit itself through the notification via the application's server. There are complaints from different users about the cracking of their mobile phone through this virus.

## **SURVEILLANCE: VIOLATION OF INDIVIDUALS' RIGHT**

The Court took a strong stand against the surveillance on individuals and said that, in a democratic society spying on individuals cannot be allowed except by following due procedures established in the Constitution with sufficient statutory safeguards. Unlawful surveillance affects the society at large and violates major rights that an individual has. First and most important right that is violated is that of Privacy because major requirement of Right to Privacy is to be free from observation, interference, and intrusion; surveillance violates Privacy in multiple ways this is because we are under continuous observation and under the Article 21 of the Indian Constitution an individual is provided an integral and Fundamental Right, Right to Privacy.

Unlawful spying also violates Right to Freedom of Speech and Expression, protected by the Indian Constitution under Article 19(1)(a); it is because surveillance submits us under the government authorities and it impacts the way in which people think and communicate with others about their opinion on social and political issues and it restricts the flow of important information in the society because many things get censored or there are chances that citizens don't speak up their minds in fear of getting caught by the State authorities.

## **INTERNATIONAL LAWS AND RIGHT TO PRIVACY**

Human Rights are the most important rights, which are made on the fundamental principle to bring freedom, justice and equality, and peace in the world, The Universal Declaration of Human Rights was adopted by the United Nations General Assembly on December 10, 1948 and The

International Covenant on Civil and Political Rights came into force on March 23, 1976. Both these Human Rights organization are applicable around the world.

Article 12 of the Universal Declaration of Human Rights protects and Article 17 of the International Covenant on Civil and Political Rights, protect and promotes Privacy of the individuals. It clearly states that there shall be no unlawful or arbitrary interference with the Privacy of an individual and that the individual has Right to the Protection against any such interference.

## **APPROACH TOWARDS DATA PROTECTION AND PRIVACY ISSUES**

The International Covenant on Civil and Political Rights is the main global legal instrument for the protection Right to Privacy. There has been recent changes around the around the world moving towards one step closer to data protection and infringement issues in consonance with right to privacy.

### ***Two of the major changes brought are as follows***

The Report released by UN Human Rights Council in 2017 was in attempt to address the responsibility of companies to respect the Privacy Rights of an individual in the digital age. It requires companies to adopt policies, procedures and remedies and conduct Human Rights impact assessments of their operation. The EU General Data Protection Regulation (hereinafter referred as GDPR) is the most important change in the regulation of Data Privacy in 20 years. The change was brought with an aim of reshaping the manner data is being handled in various sectors and likewise as the report of UN Council made companies liable for the mishandling of the personal information of the customers. In India, a detailed legislation on Data Protection is yet to come in force but it is believed that it is going to be equally stringent as GDPR is. Primary IT industry bodies such as NASSCOM and Data Security Council of India, have always backed rigorous Data Privacy for years in the country and ever since the Apex Court declared Right to Privacy being deemed as a Fundamental Right, the focus on Data Privacy and protection to enhance citizen safety and security has increased.

The Personal Data Protection Bill, 2019 was introduced in Lok Sabha by the Minister of Electronics and Information Technology, Mr. Ravi Shankar Prasad, on December 11, 2019. The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same.

The Bill governs the processing of personal data by:

- (i) Government,
- (ii) Companies incorporated in India, and
- (iii) Foreign Companies dealing with personal data of individuals in India.

Personal Data is data which pertains to characteristics, traits or attributes of identity, which can be used to identify an individual. The Bill categorises certain personal data as sensitive personal data. This includes financial data, biometric data, caste, religious or political beliefs, or any other category of data specified by the Government, in consultation with the Authority and the concerned sectoral regulator.

## **CONCLUSION**

The Government of India needs to adopt Data Protection legislation to prevent exploitation of data by public or private entities. In order to do that, the Government can regulate the treatment of personal data or information by limiting the actions of those entities to only unquestionably relative and necessary information. Although India has made certain timely amendments in IT Act, 2000, the lack of stringent and separate Data Protection Legislation has made the situation only worse. This necessitates passing of a new legislation that will deal specifically with the personal Data Privacy issues and challenges in the country. However, while drafting the legislation, caution has to be made to balance the interests of common public and to overcome the increased rate of cybercrimes so that people are not under constant fear of their personal information getting misused or leaked. In general it is considered that despite the efforts put by the government to preserve basic human rights of citizens, there always exists a question as to the possibility of myth that Privacy and Data Protection could be promised in this digital age.

## **References**

1. Report of the United Nations High Commissioner for Human Rights on, The right to privacy in the digital age
2. EU General Data Protection Regulations
3. K. S. Puttuswamy v. Union of India, AIR 2017 SC 4161
4. Basu. D.D. (2016), Constitution of India, Lexis Nexis, Butter Worth's Wadhwa Nagpur
5. Dr. Pandey J.N. (2014), Constitutional Law of India, Central Law Agency, Allahabad
6. Jain. M.P. (2014), Indian Constitutional Law, Lexis Nexis, Gurgaon, Haryana