Taming the Untamed: Data Privacy in Cyberspace

Mohd Faiz Khan[*]

Abstract: Throughout the walk of human history, one of the most cherished things that cannot be separated from a human being is the privacy of an individual. In ancient Greek, we can see Aristotle's distinction between the public sphere of life associated with politics and the private sphere related to domestic life. The term privacy can be stated as a matter of affairs that are kept beyond the reach and breach of others. It is one of those facets of life where the information regarding an individual's life, work, and those conditions that are not public is privately protected. The growth of the right to privacy is usually traced back to Warren and Brandies' view, which was published in the name of the right to privacy in 1890 and stated that "the right to life has come to mean the right to enjoy life, the right to be left alone; the right to liberty secures the exercise of extensive civil privileges". In the present era of information and technology, with the emergence of cyberspace, data privacy is the need of the hour, and it has become a hotly debated topic. In cyberspace, millions and billions of people have their data online and to keeping them safe and secure is the biggest challenge. During the COVID-19 pandemic, there has been a tremendous surge of users in cyberspace. With fast-evolving information technology and communication, data privacy has become more vital and volatile. Countries around the globe are moving in the direction of strong cyberspace protection through the implementation of various data protection laws. But in India, it is neither protected nor secured by a special national legislature. The intent of this article is to get a general idea of cyberspace along with the legal implication of data privacy.

Keywords: *Breach, Protection, Netizens, Internet.*

1. Notion of Cyberspace

The term "cyberspace" was unknown in the 19th century. With the emergence of the internet throughout the world, the concept of cyberspace comes into play. Cyberspace refers to the notional environment in which communication is done over the computer networks situated throughout the globe. It is the communication environment supported

[*] Research Scholar, Faculty of Law, Integral University

by computer networks. It is the opposite of physical space. Today, everybody in one way or the other is connected to cyberspace. With the advancement of internet accessibility and reach, the world has become a global village where everyone is connected through the internet over cyberspace. From online shopping to financial transactions, everything is being done in cyberspace. During the COVID-19 pandemic, the cyber dependency has reached a completely new level where everything was moved to virtual mode.

From corporate work to educational institutions everything went online mode. It was reported that millions of new people joined the world of cyberspace making it more open and reliable in terms of information technology and communication. As we know, great power comes with great responsibility, the same goes for cyberspace. In an environment where millions and billions of people interact and transact every minute, the security of such an environment remains significantly relevant. With the emergence of online networking, the safety and security of netizens remain paramount. In the drastic rise of online interaction and transactions, the data privacy of netizens is the most crucial topic discussed throughout the labour realm of cyberspace. Experts believe that the ultimate aim of the cyberspace regime can be achieved only when the netizens feel protected against cybercrimes by making strong firewalls across cyberspace.

2. Need for Cyberspace

With the advancement of information technology and communication, life has become faster and more far-reaching; the internet has revolutionized the life of the 21st century. It is impossible to think of a day without the internet. The internet has become a new habit of the masses and brought the whole globe a single click away as it was unthinkable in the past. Cyberspace has brought a whole new dimension to our daily life. Even without stepping out to the physical world, we can roam around the globe through virtual traveling. It has made it possible to connect to the different parts of the world irrespective of any physical barrier.

The emergence of the cyber world has removed the barrier of time and place. The far-reaching interaction and transaction have made us realize that cyberspace is not only an environment of computer networks but an essential need of the hour. With the help of the internet, today people are moving everything online. From online shopping to online banking, everything has moved over cyberspace, thus making it more advanced and effective in breaking the barrier of time consumption. One of the real advantages of cyberspace is independence from the physical world. Earlier nobody would have ever thought of online shopping, online banking, online education, etc. Today we cannot think of a world without e-commerce. The realm of cyberspace has made us too close to the globe which was never happened before. The need for cyberspace demands the strong protection of cyberspace against cybercrimes. We need strong laws and regulations to protect and make cyberspace a haven for the netizens.

3. Data – The New Oil of 21st Century

"The world's most valuable resource is no longer oil but data."[1] In the case of oil, once the oil company finds it in the ground, they know how to turn that oil into profits through drilling, extracting, refining, and finally selling. In cyberspace, the companies having big data know exactly how to make a gain out of it. They often take the wrong path to make a huge profit. That's why it is the data that is generating multi-billion dollars industry over cyberspace. Since oil is precious in terms of quality and quantity, the same goes for data.

Cyberspace deals with complex levels of data usage and transmission. Data privacy is the most challenging issue in cyberspace. Maintaining one's privacy is very essential both in the physical and the cyber world. Over cyberspace, data is so vast and far spread that it becomes a challenge to keep them safe and secure against any infringement and breach. With everything moving to online mode, it is the need of the hour to protect data privacy in cyberspace. Protecting data privacy in cyberspace is not an easy task since we cannot trust any source blindly without verification. It has come to light that many big tech giants have been involved in the data breach of their organizations knowingly or carelessly. Data are sold to different players to make huge money. Various instances have shown us that companies leak and breach big data to government or private parties in return for financial advantages.

[1] 'The world's most valuable resource is no longer oil, but data' (*The Economist*, 6 May 2017) <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> accessed 13 May 2022

4. Challenges to Data Privacy

There are various challenges related to data privacy that we come across in day-to-day life. The biggest issue with regard to data privacy is a data breach. With the increase in the commercial availability of AI-enabled devices, the rate of breaches and data loss has also increased dramatically. In the first half of 2021 alone, India suffered about INR 165 million resulting from data loss due to malware attacks. The interesting fact is that most of the compromised data belongs to big companies like Aadhar (UIDAI), Facebook, Air India, Domino's India, Unacademy, Money Control India, etc. A few of them are mentioned below.

4.1. Pegasus Spyware Controversy

It was created by the Israeli NSO Group and is known for zero-click surveillance products. It has faced numerous backlashes due to its ultimate access to any secure smartphone. Apps such as WhatsApp and Facebook use end-to-end encryption and cannot be tracked or tracked. However, NSO Group's Pegasus product breaks the encryption barrier by simply calling your number, and then you can remove it. Users can also read encrypted messages and phone calls. Pegasus spyware enters all devices through backdoors, and device owners are unaware of the presence of spyware. Once installed, it uses a zero-click exploit to collect arbitrary data from the device and give users complete control over the data.

The International Media Consortium[2] has reported that more than 300 verified Indian mobile phone numbers are on the list of potential targets for Pegasus spyware monitoring. NSO Group stated that spyware was designed solely for governments and law enforcement agencies to obtain useful and hidden information, but this fact alone does not guarantee personal privacy. The Supreme Court has raised this issue and wanted to know if the union government was using Pegasus spyware in an illegal way to spy on civilians. Many petitioners demanded an independent investigation related to reports of alleged espionage against respected citizens and politicians by government agencies using Pegasus spyware.

[2] 'False rumours: Stand by findings of Pegasus Project, says Amnesty International' (*The Times of India*, 22 July 2021) <https://timesofindia.indiatimes.com/india/false-rumours-stand-by-findings-of-pegasus-project-says-amnesty-international/articleshow/84643073.cms> accessed 17 May 2022

4.2. Aadhaar Database Breach

The largest (data breach) was in India, where the government ID database, Aadhaar, reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens.[3] It was reported in January 2018 that criminals were selling access to the database at a rate of Rs 500 for 10 minutes, while in March a leak at a state-owned utility company allowed anyone to download names and ID numbers. Between August 2017 and January 2018, Aadhaar numbers, names, email and physical addresses, phone numbers, and photos of almost 1.1 billion Indians were found susceptible to the data breach.[4]

4.3. COVID-19 Results Data Breach

In early 2021, a database containing the information of at least 1,500 Indian citizens was compromised following an attack on government websites. The hackers made the data public through downloadable PDF files. It was later discovered that New Delhi-based agencies were involved in the attack. A similar incident occurred in 2020 when the Delhi State Health Mission database was hacked and the privacy of 80000 COVID19 patients was breached. The Kerala Cyber Hackers group claimed responsibility for the attack and said the reason behind it was dissatisfaction with the way the government was treating healthcare workers.

4.4. Air India Data Breach

In March 2021, Air India announced that it suffered a data breach in the last week of February. According to the company, "the data of around 45 lakh users was leaked which included their name, date of birth, mobile number/email address, passport information, ticket information, frequent flyer data, and credit card information".[5] This was one of the gravest data breaches ever, as it also includes passport details, one of a person's most important identification documents.

[3] The World Economic Forum's (WEF), *Global Risks Report 2019*

[4] Martin Hron, 'Top 10 Biggest Data Breaches in 2018' (*Avast*, 20 December 2018) <https://blog.avast.com/biggest-data-breaches> accessed 2 June 2022

[5] DGCA, *Air India Notification of Data Breach,* 7 June 2021

4.5. Facebook Data Breach

We all know about frequent data breaches on Facebook. This social media platform is quite famous for its data leaks. In a security attack that took place in April 2021, the data of about 60 thousand Indian users was leaked on Facebook. The data breach included "Facebook ID, email ID, phone number, date of birth, location, and relationship status". Although the company claims to have fixed the problem, the dataset is said to have been posted to an online forum and is available to anyone.

4.6. Domino's Data Breach

On 22nd May 2021, it was uncovered that "data of 18 crores Domino's orders was leaked online. The data breach included name, email, mobile number, and even the GPS location of the user". Hudson Rock firm claimed that "credit card details of 10 lakh people who ordered pizza from Domino's had also been compromised.". However, Jubilant Foodworks, which owns Domino's, claimed that no financial data had been leaked.

5. Data Protection Laws

According to statistics from the United Nations (UN), 137 out of 194 countries have laws that guarantee data protection. Leading the pack in terms of rigor is the European Union's privacy regulation known as the General Data Protection Regulation.[6] The GDPR protects basic information related to identities such as name, address, ID numbers, location, cookies data, and IP address. It also safeguards health data, biometric data, ethnic data, political opinions, and sexual orientation.

The GDPR went into effect in 2018 and has since inspired similar laws around the world, including in China, New Zealand, the UK, and India. GDPR deals with data subject rights, data controller duties, supervisory authorities, remedies, liability and punishment, transfer of personal data to third parties, etc. Iceland is considered the "Switzerland of data" by many. For the collecting of personal data, the Nordic Data Protection Act of 2000 requires "explicit and informed consent". In 2018, the Chilean government revised the country's Constitution to make personal data a human right.

[6] The General Data Protection Regulation (EU)

5.1. United States

Data privacy is not as well-regulated at the federal level in the United States. The federal government, like many other things, leaves many of the specifics to the states. Laws also differ by industry, resulting in confusion of laws and regulations for website owners in the United States.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which deals with health-related information, and the Children's Online Privacy Protection Act (COPPA), which applies to websites that collect data from children under the age of 13, are two federal laws that deal with data privacy. Some states have stricter laws than others, such as the California Online Privacy Protection Act (CalOPPA), which was the first law in the United States to require websites specifically to post privacy policies and maintain confidentiality. CalOPPA applies not only to California-based Websites but to any website that collects personal data from consumers residing in California. With that in mind, US-based website owners are urged to exercise caution to avoid inadvertently getting into legal trouble. CalOPPA requires each website that collects personal data from users to post a privacy policy that includes:

Types of personal data collected in the United States:

- any third parties you share data with,
- how users can view and change the data that you have collected,
- how will you notify users of changes to your privacy policy,
- when is the privacy policy's actual date, and
- how you respond to a do not track request.

5.2. China

Two new laws in China dealing with data security and valid privacy got implemented in the fall of 2021. They not only regulate the citizens but also affect many multinational activities in China or have activities affecting China. These two laws - Data Security Act[7] and Personal Information Protection Act[8] - provide a more specificity of data positions,

[7] Data Security Act (DSL)

[8] Personal Information Protection Act (China)

export requirements for data, and data protection appearance fairy. Data Security Act (DSL) sets data classification data collected and stored in China based on its potential. Impact on Chinese national security and regulate storage and transfer based on the level of data classification.

The Personal Information Protection Act (PIPL) is the first Chinese Law of Adjustment to protect personal information and modelled after the general regulations on data protection of the European Union. "Personal information" is widely determined to cover "all information to identify or identify natural people stored in electronic devices or any other format". As long as information "relates to natural people to identify or identify", even if the information is not enough to identify a specific person, PIPL is always applied. It typically refers to any data-linked activity (e.g., collection, storage, use, reorganization, transmission download, transmission, disclose, and suppress) related to personal information of data topics in China, as well as external activities to China to provide products or services for people in China or their behaviour analysis. Violations of the PIPL can result in fines of up to RMB 50 million (~$7.78 million), 5% of a company's annual revenue, and failure of all illegal income.

5.3. United Kingdom

The Data Protection Act 2018 implements the General Data Protection Regulation (GDPR) in the United Kingdom. The Act regulates how organisations, enterprises, and the government utilise your personal information. Everyone in charge of utilising personal data must adhere to tight guidelines known as "data protection principles". They must ensure that the information is:

- used fairly, lawfully, and transparently,
- used for specific, explicit purposes,
- used in a way that is adequate, relevant, and limited to only what is required,
- accurate and, where necessary, kept up to date; kept for no longer than is required, and
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction, or damage.[9]

[9] In the UK, the mission of the Information Commissioner's Office is to uphold information rights in the public interest.

5.4. India

The Personal Data Protection Bill ("Bill" *hereinafter*) was introduced in the Indian Parliament in 2019. The idea is to lay out a system to protect personal data and define the conditions of access by public institutions and private. The Bill includes sweeping regulations on the collection, storage, and processing of personal data, and sets out penalties and compensation for violations. However, nearly two years later, the Bill has yet to become law. The Bill has also been the subject of criticism. Justice BN Srikrishna[10] criticized the revised version in 2019. He called it "an attempt to turn the country into an Orwellian state", exempting the authorities and government agencies restrict access to data.

The Joint Parliamentary Committee ("JPC" *hereinafter*) of India submitted its report on the proposed Data Protection Bill on December 16, 2021. The JPC advocated a staged strategy to implement the legislation in its report, starting with the appointment of different government authorities, such as the Data Protection Authority and completing full implementation within twenty-four months. A draft version of the Bill was also included in the JPC's report. The Data Protection Authority, an independent, autonomous, and well-resourced regulatory organisation will be responsible for enforcing data protection and safeguarding rights. The appointment and powers of the Data Protection Authority, on the other hand, contain some troubling design decisions that give the Central Government authority and influence over it.

The Bill was expected to be enacted by Parliament in its next session, with enforcement expected in the first part of 2022. But unfortunately, the Central Government withdrew the long-awaited Personal Data Protection Bill, 2019 in August 2022 to replace it with a new bill with a 'comprehensive framework' and 'contemporary digital privacy laws'. The government will bring a set of new legislation for a comprehensive legal framework for the digital economy. A statement containing the reasons for the withdrawal was circulated to the members of Lok Sabha. Reportedly, the statement included that the government was working on a comprehensive legal framework considering 81 amendments and 12 recommendations proposed by the JPC.

[10] Personal Data Protection Bill 2017

6. Conclusion

Data breaches are becoming increasingly common in modern India. As of November 2021, a study revealed that 86.63 million Indian users had been affected by the breach.[11] According to an IBM study, the average cost of a data breach in India is INR 16.5 billion, a 17.85% increase over 2020. The Indian government has had to deal with several arrests by private entities such as Facebook and Cambridge Analytica. India desperately needs a strong data protection policy, particularly that which protects individuals' data from all actors–public or private. It will need an independent enforcement body, vested with enough power and authority to ensure that such a policy is implemented in letter and spirit, with a clear goal of safeguarding the rights of the citizen. It is also important to educatepeople about the value of their data.

With the progress of Information and technology, cyberspace has become a reality of time. From small businesses to the banking sector, everything is getting online. In such a fast- moving technology, there must be strong regulations to protect individuals who are involved in such transactions. Cyberspace needs to be a haven for netizens. It is the need of the hour to protect millions of people in cyberspace through rigid rules and regulations. When done for the right reason and in a transparent manner, data protection is effective. The information gathered should be specific to the goal. There should be a limited data requirement and the website owner's accountability. There is a requirement for precision. Due to cases of privacy breaches and technological advancements, online privacy has sparked the interest of internet users. Examine your account's privacy settings on a regular basis. With someone you've never met, you could be providing more information thansimply your name and age.