JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Right to Digital Privacy and Cyber Security in India – A Legal Assessment with reference to the District of Kamrup Metropolitan, Assam

By

Dr Smita Sarmah[1]

Abstract

Right to privacy is one of the most prominent human rights of an individual which is violated very frequently due to misuse or ignorance. This right to privacy has, in the modern days, become an integral issue in the cyber space. In the recent times, most of the people have been increasingly making use of the cyber space to seclude themselves from their physical-social circle. There is a general belief that these people want to secure their privacy without interfering into another's lives. But, in reality, it has turned to be a more serious threat of infringement of privacy of an individual in the cyber space. Therefore, it has become necessary to make people aware of the unforeseen dangers they might encounter in the physical as well as digital world which might violate their privacy. In the digital world, it has become easier to infringe privacy of a person. Hence, awareness is necessary to be acquainted with the remedies available against such violation in both the physical and the virtual world. This paper, therefore, wants to highlight the concept of digital privacy in the cyberspace and the different problems connected with the violation of that right.

Keywords: Privacy, Cyberspace, Digital privacy, Infringement, Awareness, digitization.

1.1. Introduction

Privacy is a fundamental human right enshrined in many international treaties. It is important for the protection of human dignity and is one of the important pillars of a democratic country. It supports the rights of self and others.

Privacy is a right that all human beings enjoy by virtue of their existence. It also extends to physical integrity, individual autonomy, free speech, and freedom to move, or think. This means that privacy is not only about the body, but extends to integrity, personal autonomy, data, speech, consent, objections, movements, thoughts, and

[1]Assistant Professor (Senior), Department of Law, Cotton University, Guwahati, Assam, India

reputation. Therefore, it is a neutral relationship between an individual, group and an individual who is not subject to interference or unwanted invasion or invasion of personal freedom. All modern societies recognize that privacy is essential and recognize it not only for humanitarian reasons but also from a legal point of view.

The Right to Life within Article 21 of the Indian Constitution has been held to include all aspects that makes a person's life more meaningful and the Right to Privacy is one of these rights. This issue was first raised in *Kharak Singh vs. the state of UP* (1962) in which the Supreme Court of India held that 'the right to privacy is part of the right to protect life and personal freedom'. Several other judgements have followed the principle of upholding the Right to Privacy as an integral part of fundamental existence of individuals.

1.2. The current Scenario of Digital Privacy in India

The concept of privacy, in the current times, has extended itself to the cyberspace. Digital privacy in India has become a significant concern due to the increasing reliance on technology and the internet in various aspects of daily life. The Indian government has recognised the importance of protecting digital privacy and has taken steps to address it through legislation and regulatory frameworks.

In the recent case of *K. S. Puttaswamy vs Union of India* (2017)[2], the judges were unified in their belief that privacy is the constitutional core of human dignity and autonomy. The unanimous results reached by the judges in this case show that privacy includes bodily integrity, the element of mind, freedom, dignity and independence and is linked to the fundamental freedoms provided in Part III of the Constitution. Since it has been designated as a fundamental right, the State's involvement in ensuring the right is critical. The ruling of the case indicates that in future, it may so happen that many additional elements of privacy will be covered. This judgement laid down the foundation for strengthening digital privacy laws in India and has had far reaching implications of data protection and privacy rights in the country.

India is currently experiencing a 'data-based' revolution. With the explosion of digital services, India is generating a significant quantum of personal data. This collected data is being used by a wide variety of enterprises to deliver value to their users and alter their businesses. The internet traffic in India witnessed an unprecedented four-fold rise in 2021. Moreover, a recent study by MeiTY (2019) estimated the size of India's digital economy is expected to reach an unprecedented growth by 2025 in their 'business as usual' scenario.[3]

However, with the growing adoption of digital tools by citizens, issues pertaining to the extent of control, individuals have, on their own data takes centre stage. It has been recorded that 97% of Indian consumers are concerned about their data privacy, indicating a growing demand for comprehensive data protection measures. The current study has been conducted in the region of Kamrup Metropolitan district of Assam, which is an urban area, also shows the same amount of awareness among people about their digital privacy. This has in turn

[2]10 SCC 1

[3]Unlocking The Potential of India's Data Economy: Practices, Privacy and Governance, available at https://www.omidyarnetwork.in/insights/unlocking-the-potential-of-indias-data-economy-practices-privacy-and-governance (visited on 09/07/2024)

escalated the need for a dedicated privacy protection legislation in the country. While the Indian government is working towards the enforcement of a dedicated data protection legislation, several factors including hindrance to businesses, lack of awareness in consumers etc. have served as barriers to the same. However, the newly-introduced draft Digital Personal Data Protection Bill, 2022 provides the citizens of the country with the much-needed belief that India may soon join the group of nations enabling citizens to choose the manner in which their data is handled.

At present, data protection and privacy in India is primarily governed by the Information Technology Act, 2000 (the "IT Act") and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Apart from these, other sectoral ancillary regulations, aimed at safeguarding data also exist.

Although some provisions under the IT Act aim at regulating the processing of personal data in cyberspace, the primary focus of the IT Act has been on providing information security regulations for the protection of personal and sensitive data in cyberspace. The IT Act, 2000 deals with a range of issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms in respect of personal data. Moreover, the Act contains a number of provisions pertaining to safeguards against online privacy. These include but are not limited to the provisions against hacking, online frauds, monitoring, interception etc.

Further, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 provide reasonable security practices and procedures, which the body corporate or any person who on behalf of the body corporate collects, receives, possesses, stores, deals or handles information is required to follow while dealing with "Personal sensitive data or information". The SPDI Rules are not intended to be exhaustive, but require companies to have a privacy policy, follow consent requirements and inform data subjects related to the manner of use of their data.

While the IT Act and its ancillary Rules did create some extent of regulation in the data privacy space, the need for a dedicated data privacy legislation was felt within all spheres of the society. The Indian government recognised the need for robust legislation for the protection of citizens' right to privacy, while also ensuring the acceleration of the digital economy. Accordingly, a committee of experts was constituted in 2017, headed by Justice BN Srikrishna to identify key data protection issues, methods of redressal etc. The Srikrishna Committee submitted its report in 2018, along with a draft bill to tackle issues pertaining to digital privacy.

Pursuant thereto, a Personal Data Protection Bill was introduced in the Indian Parliament in 2019. This is one of the key pieces of intended legislation related to digital privacy in India, which aims to regulate the processing of personal data of individuals by government and private entities. The bill draws inspiration from international standards such as the European Union's General Data Protection Regulation (GDPR) and seeks to establish principles of data protection while balancing the interests of individuals and businesses.

The PDPB proposes several measures to safeguard digital privacy, including:

1. Consent: Individuals' consent is paramount for the collection, processing and sharing of their personal data. The bill mandates that entities must obtain explicit consent from individuals before collecting and using their personal data.
2. Data localization: The bill requires certain categories of personal data to be stored and processed only within the territory of India. This measure aims to ensure the sensitive personal data is subject to Indian laws and jurisdiction.
3. Data Protection authority: The bill proposes the establishment of a Data Protection Authority (DPA) to oversee compliance with data protection regulations, investigate data breaches and adjudicate disputes.
4. 4. Data Breach Notification: Entities handling personal data are required to report data breaches to the DPA and affected individuals promptly. This provision aims to enhance transparency and accountability in the event of data security incidents.
5. Right to data portability and Erasure: The bill grants individuals the right to access their personal data, request its portability to other service providers and request its deletion under certain circumstances.

1.3. Objectives:

(i) To find out, is the Information Technology Act, 2000, and amendment of the Information Technology Act, 2008 effective and efficient enough for controlling the recent other digital related developments regarding right to privacy in India.

(ii) To study of reaction of digital community on infringement of right to privacy.

(iii) To identify the knowledge of people on their human rights and the right to live with dignity as offered by the Constitution of India.

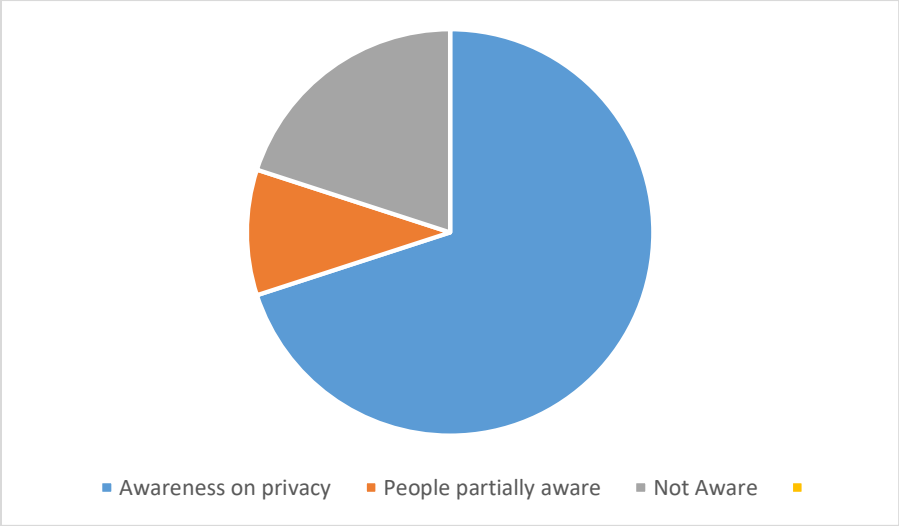
1.4. Methodology:

The researcher has adopted a mixture of doctrinal and empirical methods of data collection and analysis. Convenient sampling has been used to collect data from 300 respondents through interview and questionnaires.

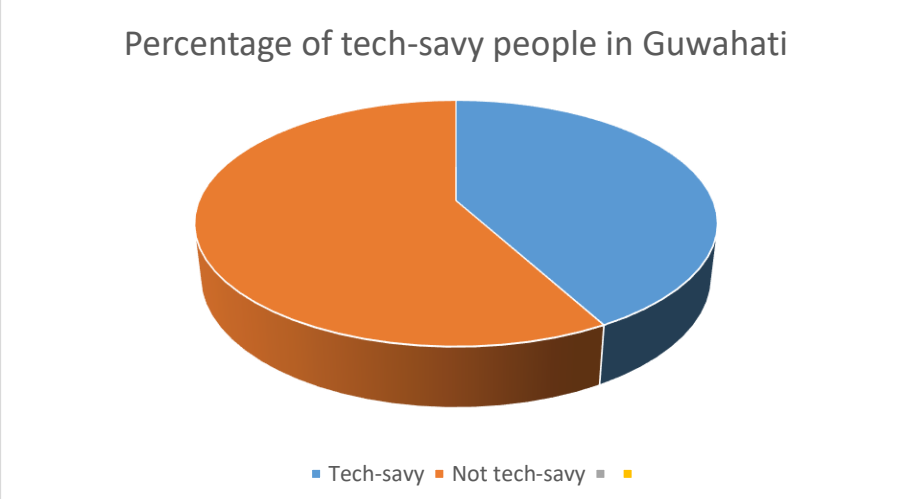
1.5. Results and Discussions

The researcher took the District of Kamrup Metropolitan as an area of survey. 300 people were interviewed and questionnaires were also distributed to find out their opinions towards protection of digital privacy. As a result of the survey it was found that:

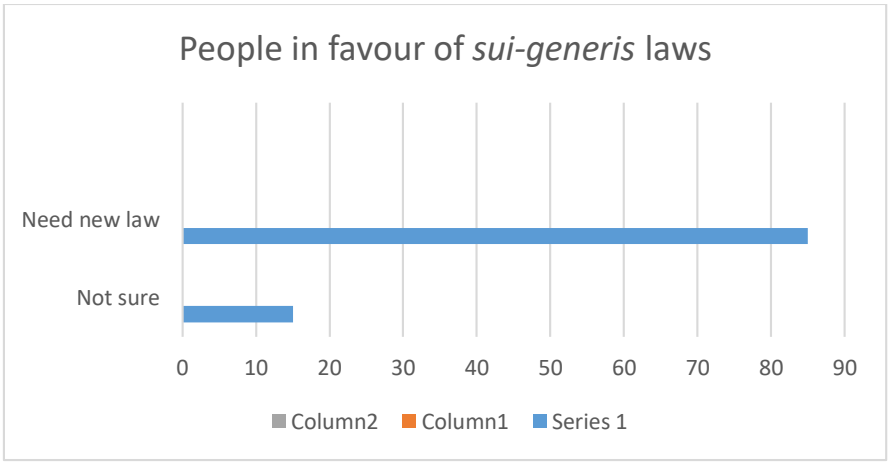
1. In the District of Kamrup Metropolitan, Assam, 70% people are aware and concerned of their right to privacy.



2. 80% people are concerned about security in relation to making purchases or banking over the internet.
3. 90% people prioritise privacy over convenience.
4. People are in support of a robust law to protect privacy in India.
5. A good number of people (almost 42%) in the region are not tech-savy and are prone to violation of privacy while using smart devices.



6. In this paper, the first objective was to find out, whether the Information Technology Act, 2000, and amendment of the Information Technology Act, 2008 are effective and efficient enough for controlling the recent digital privacy issues and other related developments regarding right to privacy in India. It was found out that only on the basis of that one law, violation of digital privacy cannot be safeguarded. India is in urgent need of more and updated cyber laws which will specifically cover issues like this and which will be applicable to the upcoming unknown digital problems.



7. The second objective was to study the reaction of digital community on infringement of right to privacy. It was found that in the district of Kamrup Metropolitan, which is an urban area, people are more or less aware of the infringement of their rights to privacy or the possibility of that as they are very commonly using digital platforms for most of their works. People are using these platforms without having proper digital literacy which is a matter of concern.

8. The third one was to identify the knowledge of people on their human rights and the right to live with dignity as offered by the Constitution of India. It was found that the people are partially aware of their human rights but the Constitutional provisions are also not upgraded to cover digital privacy.

1.6. Recommendations

On the basis of the survey made and the documents studied by the researcher some recommendations can be put forward which might be tried by the authorities in the process of protection of digital privacy in India:

(a) Harmonise the legal framework which regulate communications surveillance in India to ensure that the law is accessible and clear, and meets India's international human rights obligations;

(b) Establish an independent and effective oversight mechanism with a mandate to monitor all stages of interceptions of communications to ensure they are compliant with India's domestic and international obligations to respect and protect the right to privacy and other human rights;

(c) Establish independent accountability mechanisms and clear standards for India's security and intelligence agencies to ensure they are subject to independent oversight mechanisms and guarantee transparency of their mandate and operations in accordance with international human rights standards;

(d) Review and reform the regulations regarding export and import of surveillance technologies to and from India;

(e) Review all licensing agreements which impose obligations on the private sector to facilitate and/or conduct communication surveillance, and take the necessary measures to ensure that the private sector – in both policy and practice – comply with international human rights law and standards;

(f) Review the proportionality of data retention requirements placed on telecommunications companies;

(g) Adopt and enforce a comprehensive data protection legal framework that meets international standards, applies to both the private and public sector, and establish an independent data protection authority that is appropriately resourced and has the power to investigate data protection breaches and order redress.

It has become very essential to adopt new *sui generis* law on digital privacy in India as people in the country are not technologically educated and they do not have access to awareness also. Without having knowledge on the use of electronic devices they are using them indiscriminately and have fallen prey to different cyber crimes and torts. It is high time that the people are to be sensitised and trained in using electronic devices to save themselves from emerging cybercrimes. Clearly, privacy is an emerging and increasingly important field in India's internet society. As companies collect greater amounts of information from and about online users, and as the government continues to seek greater access and surveillance capabilities, it is critical that India prioritizes privacy and puts in place strong safeguards to protect the privacy of both Indians and foreigners whose data resides temporarily or permanently in India.

References

1. Bhandari Vrinda & Sane Renuka (2018), *Protecting Citizens from the State Post Puttaswamy: Analysing the Privacy Implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018,* 14 Socio-Legal Review 143.

2. Diego Guido Noto La (2016), *the Internet of Citizens: A Lawyer's View on Some Technological Developments in the United Kingdom and India,* 12 Indian Journal of Law and Technology 53.

3. Institute for Prospective Technological Studies: Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview. Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, EUR 20823 EN, p. 14.

4. Kalra Varun, and Jain Ramisha (2017), *An Armistice between right to Privacy and Right of Surveillance, 4 Indian Journal of Law and Public Policy 1-23.*

5. Kevin Cronin P & Weikers N Ronald (2004), Data Security and Privacy Law: Combating Cyberthreats, Thomson-West, New York, at 1-49

6. Kukreja Dhiraj (2017), Securing Cyberspace, 2 Liberal Studies, 59-68.

7. Ludri Dr Amit (2010), Law on protection of personal & official information in India, The Bright law house, New Delhi, 1st Edition

8. Schwartz P, Solove D (2014), *Reconciling personal information in the United States and European Union*, 102 Calif L Rev 877-916.

9. Solove D, Hartog (2014), *The FTC and the new common law of privacy*, 114 Colum L Rev 583-676.

10. Kalra Varun, and Jain Ramisha (2017), *An Armistice between right to Privacy and Right of Surveillance, 4 Indian Journal of Law and Public Policy 1-23.*