LEX IS US LAW JOURNAL

VOLUME 2 AND ISSUE 1 OF 2023

INSTITUTE OF LEGAL EDUCATION

Lex is Us Law Journal

(Free Publication and Open Access Journal)

Journal's Home Page – https://liu.iledu.in/

Journal's Editorial Page - https://liu.iledu.in/editorial-board/

Volume 1 and Issue 1 (Access Full Issue on - https://liu.iledu.in/category/volume-1-and-issue-1-of-2023/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

LEX IS US LAW JOURNAL
Volume II and Issue I of 2023
ISBN - 978-81-960384-0-3

Published by
Institute of Legal Education
https://iledu.in

CYBERSPACE ISSUES ON PRIVACY

Author - PRACHI SHUKLA, STUDENT OF S. S. KHANNA GIRLS' DEGREE COLLEGE, UNIVERSITY OF ALLAHABAD

Best Citation - PRACHI SHUKLA, CYBERSPACE ISSUES ON PRIVACY, *LEX IS US LAW JOURNAL*, 2 (1) of 2023, Pg. 43-48, ISBN - 978-81-960384-0-3.

ABSTRACT

21st century undoubtedly, has become the era of digitalization, carving a whole new world out which we refer to as 'virtual world/ cyberspace'. The term IT signifies the technological and scientific aspects alongwith the management used for the purposes of handling the communication, data and it's processing, application of entailed software and so on. Thus, IT consists of 4 main essentials:- hardware; software; people; and their data. Cyberspace connotes a connection of various computer networks through electronic medium wherein individuals communicate, interact, present ideas, carry-out businesses, online transactions, upload and download software, share information, etc. through an online platform. Cyberspace, in whole, is a virtual world which has no physical existence and where people can connect easily through a computer, PC or their mobile phones and internet. Consequently, this era is witnessing the explosive expansion of the boundaries of cyberspace and it won't be wrong to say that the ever-evolving IT and Information & Communication Technology are responsible for the same. As the cyberspace has no physical existence like the real world, it has become much easier for anyone to commit any wrong or malicious act and still remain anonymous. Although the information, communication and technology together have proved to be a milestone towards making a whole new virtual world, but ironically the capabilities of the digital arena to collect information, storage of data, processing, etc. have made the users vulnerable to one of the major kinds of cybercrimes i.e., 'invasion over their privacy'. This article aims to go through various threats/ challenges to privacy in cyberspace in the context of India, and analyze the legal provisions to combat this issue in India.

KEY WORDS:- Cyberspace, cybercrime, privacy, legislative provisions, Digital Personal Data Protection Bill, 2022.

Introduction

The emerging world of Information and Communication Technology has paved the ways of worldwide communications and feasibly available information. Cyberspace neither has a tangible existence, nor it has any such limitations like boundaries/ geographical extent and so it is widening its reach every day. Also, this space which we refer to as 'cyberspace' has no complicacies in regard of entering and exit, which means that everyone and anyone can gain access into the virtual world with an anonymous or impersonified identity with the minimum probability of being caught. With the advent of modern world stepping-in to the digital era, mankind is now totally dependent on the Information Technology and computers in some way or the other and which consequently makes the users vulnerable to a number of cybercrimes. The unlimited freedom on internet and the capacity of the hi-tech networks to collect, storing and processing the data (i.e., personal information) has become seriously a grave threat to the security of the individuals all over the globe. The giant figure of the number of people surfing the internet and being active on social-media sites, sharing and posting about their day-to-day

LEX IS US LAW JOURNAL
Volume II and Issue I of 2023
ISBN - 978-81-960384-0-3
Published by
Institute of Legal Education
https://iledu.in

personal information, pictures, videos, etc. has exposed their privacy to the perpetrators at a severe level which is unimaginable.

Privacy is the basic right of the human but the large amount of private, sensitive, personal information of the users/ individuals captured in the web of digital platform breaches this basic human right as well. In India, Article 21 of the Constitution of India entwines shield to the 'right to privacy' within the parlance of fundamental rights and protects the dignity of the individuals. A separate legislation to deal with the cyber world, cybercrime and electronic commerce has its existence in India i.e., The Information Technology Act, 2000. In the case of Sanjay Dhande v. ICICI Bank & Vodafone, 2014 Sanjay's bank account was hacked and a handsome amount of 19 lakh rupees was withdrawn from it alongwith blocking his SIM card so that he doesn't get notified about the transactions. The court in this case held that the data that is held by the telecom companies is, according to Section 43A of the IT Act, 2000, "sensitive personal data"[34]. The Supreme Court, through its aadhaar card judgement i.e., in the case of Justice K. Puttaswamy v. Union of India, 2017 opined that the right to privacy includes within its ambit the 'privacy of information' in regard of data protection under the IT Act, 2000. The government, through this Act tried to focus on the protection of the user's privacy in digital aspects but even after several amendments in this Act there still exists a need for a separate law which specifically concentrates on privacy on the internet. There remains a need of such security measures, procedures and privacy laws in reference to the cyberspace, which has the potential to reduce the risk of setting-in to a user's privacy through gathering information, storage and leakage of personal and private data.

Cyberspace is that digital world of computer and internet wherein every single click by the user leaves the user's footprint at that very moment in that particular space, without his knowledge. Thus, it is a matter of great concern. The social media, credit card agencies, service providers, etc. hold sensitive information about the users through the digital platform. Everything is so effortlessly accessible in the digital space that anyone can access any sort of data or information about anyone at any point of time, thereby, raising grave issues of privacy breaches of individuals and organizations / institutions in the modern world.

I. Major Threats/ Challenges to Privacy in the Cyberspace in India

:- The various threats are categorized under the following heads:-

(A) Cyber Snooping:- Snooping refers to tracking the activities of an individual by means of any utility or any program which performs the function of monitoring in computers. Snooping in network security is a technique where criminals of the cyber world gain unauthorized access to an individual's information and data, which ultimately destroys the privacy of individuals by keeping such a spying eye on all those private data, financial details and passwords which might have been stored or entered in the individual's computer network/ other system device. For remotely monitoring the activity on a computer or mobile phones, or other network device, this technique makes use of software programs. Most of the time, the users are unaware of this cybercrime and if the system security network is not encrypted then the data within the system network can be read or heard through a snooper.

(B) Cyber Spoofing:- Spoofing is another technique of committing cybercrime in which messages are sent by the criminals of the cyberspace who pretend to be real and genuine, to the individuals, from a fake email address, so that the source of origin of that spam email remain unidentified. Generally, spoofing is done through E-mail. Keeping a note of this, now-a-days many e-mail servers have adopted such security features that prevent

[34] Dr. Ashok K. Jain, Cyber Law (Information Technology Act) 72 (2018-2019).

LEX IS US LAW JOURNAL
Volume II and Issue I of 2023
ISBN - 978-81-960384-0-3
Published by
Institute of Legal Education
https://iledu.in

criminals from sending spam messages. The other method by which spoofing is done is through IP address, by creating a fake IP address of a computer so that the computer source from where the data is being generated remains anonymous. The telemarketers also perform this spoofing activity by displaying the fake contact number or the area from where they are calling.

(C) Website/ Web Defacement:- Web defacement is considered as an attack on a website wherein the attackers, also called 'defacers', change the website's original content and its visual appearance. These defacers add such contents on other's website or webpage, related to any social, political and other religious matters, that has no relevance to the original matter of the webpage. This cyber offence is committed with the intention to cheat the innocent users whosoever visits the website/ the webpage. It is also one of the kinds of cyber tort.

(D) Cyber Stalking:- The term 'cyber stalking' refers to stalking through a virtual or electronic medium, in which the cyber stalker's behavior is threatening and involves unwelcome advances or harassment of any individual where that individual's chats, email, message areas, GPS technology, etc. are used by the cyber stalkers to target their victims. Females, children and those who are not emotionally strong, are the target groups for cyber stalkers. The first case of cyber stalking in India was the case of Ritu Kohli, though the offender was booked under Section 509 of IPC[35]. In India, there are no separate laws for cyber stalking and even the IPC and IT Act does neither anywhere deal specifically in cyber stalking nor define the same.

(E) Copyright Infringement:- Any person with a computer/ mobile/ any other electronic device, can have access to the internet at any time. Internet also serves as a medium for distribution of not just information but also pictures, videos, audios, and music and this even leads to easily downloading someone's original work without that person's due permission or license. The price of distribution is so less that it remains almost negligible. An individual's copyright over any work gets invoked immediately upon the creation of that work or as soon as the work is expressed in a material form. Legally, the protection of copyright is provided by the government to the creator or author of the work, upon which the author becomes entitled to many exclusive rights regarding his copyrighted work under Section 14 of the Indian Copyright Act, 1957. To be specific, neither the Indian Copyright Act nor the Copyright, Designs and Patents Act, 1988 provide for the definition of "digital work" or deal with "digital work". Going by the principles of this Act, the person/ the owner with an identity, who creates any work on the digital platform shall be the author of that digital work and shall possess all those rights of an author that are provided under Section 14 such as- making derivative works, right to publish the work, copying the work, etc. Thus, any infringement regarding any of the rights of the author, in respect of his 'work on the internet' shall be construed as copyright infringement.

(F) Phishing:- Very often, we see an email or a general message on our computer or devices or mobile phones where it seems to have been sent by a legid and authorized party/ institution/ association which mentions that we are urgently required to update our passwords, username, credit card credentials, etc., and for this we are asked to click on the link or open the attachment that has been sent through that mail or in the message box. As soon as we open the attachment or click on the link, all our sensitive information like- passwords, username and other login credentials goes in the hands of frauds. Also, such links, that pretend to be coming from a legitimate association, have the chances of being infected by malware. SIM card cloning and unauthorized use of someone's digital signature in electronic contracts also comes under the purview of

[35] Dr. Ashok K. Jain, Cyber Law (Information Technology Act) 232-233 (2018-2019).

LEX IS US LAW JOURNAL
Volume II and Issue I of 2023
ISBN - 978-81-960384-0-3
Published by
Institute of Legal Education
https://iledu.in

phishing. Basically, phishing is a type of identity theft which constitutes the crime of impersonating other person/ association on an electronic medium for financial gain. In the amended IT Act, 2000 Section 66C provides that "fraudulent or dishonest" use of other's login credentials or electronic signatures, etc. constitutes an offence, punishable up to 3 years of imprisonment and fine up to Rs. 1 lakh. Section 66D provides that "cheating by personation" through a computer system or any device constitutes an offence, punishable up to 3 years of imprisonment and fine up to Rs. 1 lakh.

(G) Vishing:- Vishing is the combination of voice and phishing, wherein a robotized/ mechanized phone call or what's app audio message is used as trap with the intention to extract sensitive details regarding bank accounts or ATM of the potential victim, often by motivating them to claim the prize money. These phone calls state that there is some issue with an individual's bank records or that the ATM card of that individual needs to be reactivated, so that the receiver, as soon as possible, indulges in the required process, ending up by providing these fraudsters with his sensitive financial bank details/ ATM card details.

II. Legal Provisions to Combat the Issues of Privacy in Cyberspace in India: Analysis:-

There is no law exclusively dealing with an individual's privacy rights regarding cyberspace in India, yet. The IT Act, 2000 deals with cybercrimes and renders the remedies for the same. Also, the Act contains some provisions in connection to an individual's privacy but they are non-exhaustive. Although, the courts in India, at many times, have interpreted the term "data protection' in the ambit of an individual's right to privacy under Article 19 and 21 of the Constitution of India. Till date, India does not have any separate law that specifically or particularly provides for "data protection". The Ministry of Electronics & Information Technology has appointed a committee of experts, which is being headed by the former Supreme Court Judge- Mr J. BN Krishna, to draft a separate law on data protection.

(A) The Constitution of India, 1950:- The Constituion of India neither exclusively provided any definition of the 'right to privacy', nor does the Constitution acknowledged it as a fundamental right. But inferences for this noble right were drawn from right to personal liberty under Article 21. Right to privacy is not an absolute right as it is subject to restrictions, on the basis of public interest. Thus, it will not be wrong to say that the 'right to privacy' has been derived time-to-time from Article 19(1)(a), Article 19(1)(d) alongwith Article 21. The judgement delivered by the Supreme Court in the case of J. K.S. Puttaswamy vs. Union of India in 2017, also known as the "aadhaar card judgment", recognized the right to privacy as a fundamental right.

(B) The Information Technology Act, 2000:- Many privacy-centered provisions were inserted in the IT Act by the amendment of 2008. In the IT Act, 2000 Section 43 provides for penalty and compensation for damage to computer and computer system, Section 66 makes provision for offences related to computer, Section 66C provides provision against identity theft or hacking, Section 66D deals with punishment for cheating by personation through a computer resource, Section 67C makes provision for retention and preservation of information by intermediaries, Section 69 envisages the powers to issue directions regarding interception/ monitoring/ decoding information through any computer system, Section 72A provides that disclosure of information with the intention and knowledge and without that individual's consent, in breach of lawful contract, is punishable with imprisonment up to 3 years and a fine up to Rs. 5 lakhs. The provision of Section 72A was added by the amendment Act of 2008. This Act however, does not deal

LEX IS US LAW JOURNAL
Volume II and Issue I of 2023
ISBN - 978-81-960384-0-3
Published by
Institute of Legal Education
https://iledu.in

with the real challenges to privacy in cyberspace and merely provides us with just a hand full of scattered provisions that render only the punishments for unlawful access to data and few rules against informational trespass. The Act nowhere defines the term 'personal data'. Also, the IT Act, 2000 as a statute of technological arena fails to provide the basic security standards in respect of 'personal data'.

(C) The Data (Privacy and Protection) Bill:- Justice BN Krishna committee was appointed to pitch-in a draft of data protection framework, to identify the challenges and possible statutory protections for the same in the light of "data privacy". As the Data (Privacy and Protection) Bill of 2017 as well as of 2019 highlight the evolving issues of privacy in the cyberspace, it won't be wrong to say that this bill has the potential to provide right to privacy in cyberspace as a statutory right. However, the draft- Personal Data Protection Bill, 2019 was withdrawn after the review owing to the need of 80 amendments and several other recommendations into it, in order to be properly presented as a well proposed draft.

In the constant efforts to bring up a comprehending data protection framework in India, again, the most awaited draft- Digital Personal Data Protection Bill, 2022 (DPDP Bill) has been released in November 2022. This Bill aims that the digital personal data be processed in such a way which considers both-

(i) a person's right to protect his/ her personal data,
(ii) the urge of processing personal data for purposes that abide by the law.

In this Bill the term "data" refers to the facts, information, details, etc.; "personal data" refers to any such data that belongs to an individual or the data is related to him in such a way that it reveals his/ her identity; "digital personal data" refers to any data which is gathered and then digitalized later as well as the data gathered via internet. The Bill excludes such personal data which has been or might be processed by a person for domestic purposes; and the data whose offline processing is done. Although, the DPDP Bill is applicable only to a digital personal data that has been or that would be processed within the territories of India. But this Bill would also apply to such digital personal data that has been or would be processed beyond the boundaries of India, only if the personal data processed- firstly, particularly examines the aspects regarding the attributes of an individual in our country; secondly, offers goods and services to the individuals in India[36].

Conclusion

The digital revolution going on throughout the world has raised the level of concerns in respect of ever-booming offences in the digital space, especially the offence of invasion of one's privacy in the cyberspace. Privacy in cyberspace is the basic necessity of each individual/ netizen (i.e., the citizens of a country using the cyberspace) so that they don't encounter any sort of invasion or interruptions in respect of personal data and information. The rapid and unprecedented advancement of technology in the field of information, communication, software, and applications makes the sense that the netizens also have to be techno-savvy, in order to stand strong for themselves against any intrusion in their privacy in digital space. Protection of an individual's privacy often also depends upon the type of information that the individual chooses to share on the online platform. However, the information, communication and technological jurisprudentia also need to have a sharp and strong captivity over the legal arena regarding cyber laws and specifically

[36] Ashneet Hanspal, Aditi Mendiratta, Gaurav Bhalla, Analysis of the Digital Personal Data Protection Bill, 2022, Ahlawat & Associates (Jan. 4, 2023), https://www.mondaq.com/india/data-protection/1267190/analysis-of-the-digital-personal-data-protection-bill-2022.

regarding the 'protection of personal data in cyberspace' in the context of India. Thus, the legislature also has to be well-acquainted at the time of formulating the laws and enactments, in order to maintain the balance amid- protecting rights and providing much needed laws to the netizens, and actively taking strict actions against the growing regime of crime in the cyberspace.

References

(1) Indu Sharma, M. Afshar Alam, "Privacy & Freedom Issues in Cyberspace with Reference to Cyber Law", Jamia Hamdard University, New Delhi-62, International Journal of Computer Applications (0975-8887) Vol. 145- No.3, July 2016.
(2) Article on "Types of Cyber Crime and Prevention", Aug. 8, 2022, https://www.vidhikarya.com/legal-blog/types-of-cyber-crime-and-.prevention.
(3) Shubhang Gupta, article on "Importance of Data Protection and Privacy Policies in Cyber Law", March 29, 2020, https://www.google.com/amp/s/blog.ipleaders.in/data-protection-and-privacy-policies-in-cyber-law/%3famp=1.
(4) Salai Varun Isai Azhagan, article on "Copyright Infringement on the Internet", March 24, 2017, https://www.google.com/amp/s/blog.ipleaders.in/copyright-infringement-on-the-internet/%3famp=1.
(5) Ashneet Hanspal, Aditi Mendiratta, Gaurav Bhalla, article on "India: Analysis of the Digital Personal Data Protection Bill, 2022", Jan. 4, 2022, https://www.mondaq.com/india/data-protection/1267190.
(6) Dr. Ashok Jain, "leading case on- Sanjay Dhande vs. ICICI Bank & Vodafone [Adjudicating Officer, Mumbai,]", in book: Cyber Law (Information & Technology Act), Publisher: Ascent Publications, 72.
(7) Dr. Gagandeep Kaur, "Privacy Issues in Cyber Space", University of Petroleum & Energy Studies, Uttarakhand, SSRN Electronic Journal, DOI: 10.2139/ssrn.3673665, Jan. 2020.