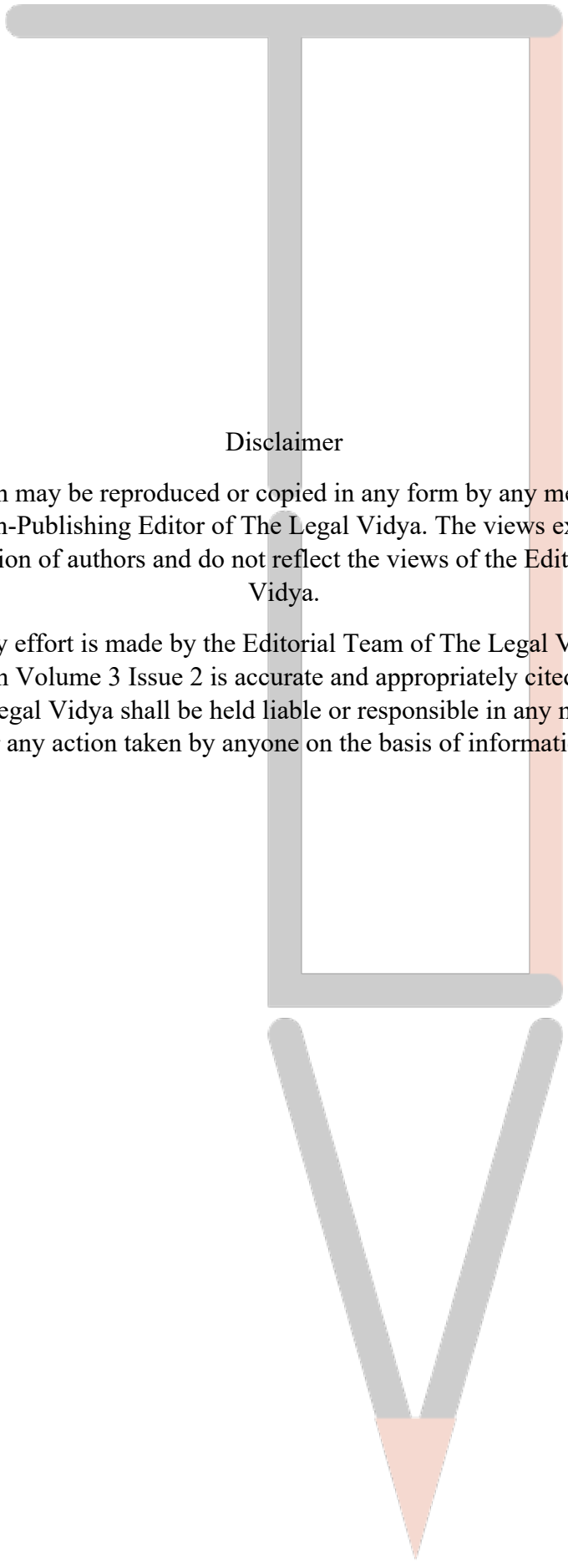
DATE OF PUBLICATION
13.04.2024

THE LEGAL VIDYA

ISSN (O) : 2583 - 1550

VOLUME 5, ISSUE 1
THELEGALVIDYA.IN



Disclaimer

EDITORIAL BOARD

MS. SHIVANGI SINHA
EDITOR-IN-CHIEF
Assistant Professor, New Law College, BVDU, Pune

"Ma'am is an Assistant Professor in Bharati Vidyapeeth New Law College, Pune. She has been a former Advocate at the Jharkhand High Court and has her specialisation in Corporate Laws. Ma'am has numerous publications and is an ardent researcher. With an inclination towards researching and writing upon Grey areas of Law, ma'am believes students shall look into matters which would help the existing and upcoming lawyers in a practical manner. In her opinion, students should be focused on prioritizing things in life. They should do things with full zeal and vigour. Her message for the students is something which she herself preaches, 'Live Your Today.'"

MR. ANKIT AWASTHI
Assistant Professor
Hidayatullah National Law University, Raipur

"Sir is an Assistant Professor in Hidayatullah National Law University, Raipur. Through his teachings, he wishes to instil in students the skill to extract relevant material from the numerous resources available these days. Sir feels it is important for students to research in the field of law which have contemporary relevance.

Sir wishes the students to put in efforts to provide an InfoBase which would be a guiding force to all the researchers."

DR. AVNISH BHATT
Assistant Professor, Xavier Law School

"Sir firmly believes that key factors for a student to excel in any profession is honesty, transparency and hard work. Law being a dynamic field, various areas of research are open to students. Students shall be creative and think out of the box while deciding their research topic. With the right amount of creativity and intellect, one can master the art of writing.

MS. RICHA DWIVEDI

Assistant Professor, Symbiosis Law School, Pune

"During her tenure as an academician she comes across students with brilliant ideas but what lacks is the research. She emphasises on the importance of substantiating views as a student of law and not just opiniating. In Ma'am words research itself suggests searching the already searched. Therefore, the research of the students shall reflect their interest in the topic. She strongly believes that a topic to be researched upon shall have contemporary relevance."

MS. NUPUR KHANNA

Assistant Professor, Christ Academy Institute of Law

"Ma'am is an Assistant Professor in Christ Academy Institute of Law. She believes that for someone to excel in a professional course like Law one is expected to focus not only on the textbook knowledge but should also focus on shaping their overall personality by participating in extracurricular activities. As per ma'am most of the students are of the view that they can take benefit only from Moot Courts, competitions, however, any activity in which you participate will help you in your professional development. Just like learning calligraphy helped Steve jobs in creating apple's typography.

Ma'am urges the young researchers to focus on the topics which are innovative and most importantly any field which interests their legal acumen.

Ma'am says that that research is at a very nascent stage in India, especially in the field of law and wishes to students that they should start focusing on improving their research skills and publishing quality papers."

ABOUT US

The Legal Vidya is a student(s) initiative run online journal (Two Issues Per Year) started in 2020 with the aim of reaching youths of the nation, buddying lawyers, students and academicians to bring forth the legal knowledge at your fingertips.

We are here to provide you with a lucid way of learning law with the help of daily blogs pertaining to the latest/other legal issues going on in the country.

We also provide legal advice and needed legal awareness to the masses with a pioneering objective of reaching the underprivileged and serving the idea of Free Legal Aid to them. (Article 39A of the Constitution of India).

We would be apprised to welcome blogs from the readers too. Readers can submit their blogs at thelegalvidya@gmail.com.

Frequency Of Publication: Two Issues Per Year
Language: English
Start Year: 2020
Format Of Publication: Online

THE LEGAL VIDYA
ISSN (O) : 2583 – 1550

Open Access Law Journal

The Legal Vidya
Volume 5 Issue 1, April, 2024, Page Nos. 36 to 71

A CRITICAL ANALYSIS OF CYBER SECURITY LAWS IN INDIA WITH RELATION TO PRIVACY AND DATA PROTECTION

MS. HIMANSHI CHHATARAM PARWANI
Student, Unitedworld School of Law, Karnavati University, Gandhinagar

INTRODUCTION

The word "privacy" has a Latin root called "privatus," which means "separated from others, deprived of something, office, or participation in governance." The objective of Article 21 of our Indian Constitution is to ensure that everyone lives in peace, dignity and freedom, and privacy is the best way to do this. Data Security and Data Protection, which are crucial components in terms of privacy as your internet activity grows, are a national issue as well as a national right to ensure as our country moves gradually towards digitalization[1] and into what is not incorrectly referred to as a "Cyber Era." Moreover, data protection and privacy are closely interwoven, and they currently occupy a highly important and delicate area in the legal system.

Data privacy and confidentiality concerns are receiving more attention than ever before because of the growing use of the internet, which exposes sensitive personal data to new security dangers. The rapid processing of large data sets, made possible by the availability of "big data "technologies[2], accelerates the immense data collection. However, combining different databases could make it possible for those who own these datasets to extract sensitive information. This issue is made worse by the pervasive data collection from many devices and data sources, like computers and Smartphone's.

The inherent risk poses a significant difficulty in this context, especially data misused by people with access to data for organizational purposes and thus the requisite authorizations to access sensitive or private data. However,

[1] Yashraj Bais, '*Privacy and Data Protection in India: An Analysis*' (2021) 4 (5) IJLMH pg. 1793–1804 <https://ijlmh.com/paper/privacy-and-data-protection-in-india-an-analysis/> accessed 23 Dec 2023

[2] Jain.P.Gyanchandani, M& Khare, 'Big Data Privacy: A Technological prespective and Review' (2016) Journal of Big Data 3(25) <https://journalofbigdata.springeropen.com/articles/10.1186/s40537-016-0059-y> accessed 23 Dec 2023

data security goes further in data privacy and confidentiality[3]. Data integrity is important because it is frequently used for important decision making. Data must be protected from illegal access. Strategies for contented authentication mechanisms are vital to achieving data security and privacy[4]. The terms "privacy" and "rights" have been defined differently by different researchers.

The definition of privacy given by **Black's Law** Dictionary is the "*right to be left alone; right of a person to be free from unwarranted publicity; and right to exist without unwarranted intervention by the public in things with which the public is not necessarily concerned.*"

Privacy is unquestionably an inherent right; it offers several advantages while also leading to exceptions. The line between privacy and confidentiality is one that we resist breaching. Consequently, it is simple to conclude that everyone has established personal privacy boundaries for the tasks they face throughout their sphere of life.

The right to privacy is now generally acknowledged to be a crucial component of Article 21 right to life and personal liberty. According to a broad interpretation, the right to life guaranteed by Article 21 encompasses more than only animal existence and the need for survival. The right to privacy is just one of the elements that enhance a man's sense of purpose, fulfillment, and worth living. The freedom to be alone is the right to privacy. A citizen has a right to safeguard the privacy of their personal life, family, marriage, procreation, motherhood, and education, among other things.

According to **D.D. Basu**, "*The term privacy is too broad, and it encompasses not only seclusion from neighbors. It can be considered as a circle around every person that no government should be allowed to cross.*"[5]

As the definitions show, there is disagreement among academics and legal experts over what constitutes privacy. The concept of the right to privacy, however, can be summed up as follows:

1. Every person has a fundamental desire for a private area where he may be confident of being free from outside intrusion.
2. Different cultures, traditions, civilizations, and nations have different ideas about privacy.

Indian intellectuals and western thinkers define privacy differently, with western thinkers viewing the right to privacy as a collection of rights. Indian academics, however, feel that privacy is a singular term that primarily refers to exclusion.

[3] Christopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey, Christopher Millard, 'The rise of cyber security and its impact on data protection' (2017) 7(2) *International Data Privacy Law*, <https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3634&context=facpub> accesssed 23 Dec 2023

[4] Mohd Satar, Siti &Hussin, Masnida&Zurina, Mohd Hanapi& Mohamed, Mohamad A, 'Data Privacy and Integrity Issues Scheme in Cloud Computing: A Survey' (2018) International Journal of Engineering and Technology(UAE) <https://www.semanticscholar.org/paper/Data-Privacy-and-Integrity-Issues-Scheme-in-Cloud-A-Satar-Hussin/> accessed 23 Dec 2023

[5] Basu D.D, *Commentary on the Constitution of India* (9th Edn, LexisNexis India, 2015)

ORIGIN AND HISTORICAL EVOLUTION OF CONCEPT OF PRIVACY

Despite being as old as humanity, privacy did not become a commonly acknowledged right until the 20th century. The innumerable religious and political literature that has been created around the world makes this evident. For instance, in India, the Arthashastra specifies architectural rules for homes based on the requirement for seclusion. These rules specify that a person's residence must be built far enough away from neighboring houses. He should also make sure the windows and doors are protected.

The Yajnavalkya, Samhita, and Manusmriti's prohibition of using someone else's property without their agreement is another illustration of the value ancient people placed on one's right to privacy in one's space and possessions. Additionally, when the Arthashastra recommended designating forest places for meditation leading to self-actualization, it provided freedom of mind. The Hammurabi Code of ancient Mesopotamia prohibited trespassing into someone's home without authorization. Roman law also prohibited entering another person's residence. However, privacy was defined quite specifically in those prehistoric times. Even research on animal behavior and social structure raise the possibility that man's quest for seclusion has animal roots.[6]

IN MODERN ERA DEVELOPMENT OF CONCEPT OF PRIVACY

Depending on the political structure in place in each nation, modern societies have different ideas about privacy. The political system has a significant impact on how the State conducts its surveillance and privacy programmes. From democracies to totalitarian states, modern nations can be grouped along a continuum. A study of privacy across the many cultures on this continuum reveals how political systems decide what constitutes private.

In nations that tend toward totalitarian systems, the government conducts extensive monitoring. As observed in China and Russia, the government is likewise exceedingly secretive about its internal operations. These States reject the individualism thesis and always put needs of the state above those of the person. So, in these countries, espionage, eavesdropping, and the collecting of private information about persons have become commonplace.[7]

Democratic States rely on individualistic ideology, in contrast to those whose inclinations are more toward the totalitarian end of the spectrum. Individual rights typically take precedence over those of the state. Since individual rights are given precedence in democracies, privacy rights have developed into a basic human right in modern cultures. So, whereas disclosure and monitoring for the sake of State objectives are unavoidable under totalitarian

[6] Alan F. Westin, '*Privacy and Freedom*' (1968) 25(1) Washington and Lee Law Review <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20> accessed 23 Dec 2023

[7] Margaret Mead, 'Child-training Ideas in a post-revolutionary context: Soviet Russia', in Margaret Mead and Martha Wolfenstein (eds.), *Childhood in contemporary Cultures*, (1955) pg 190-191 University of Chicago Press

regimes, individual and group privacy is a must for contemporary democratic States.

Cyberspace is a web (virtual space) made up of communication networks, consumer devices, and computers that connect people to the rest of the world. Cyberspace typically consists of a massive computer network made up of numerous global computer sub-networks that communicate and exchange data using the TCP/IP protocol. Cyberspace is a made-up world enabled by the Internet's network of interconnected computers. Cyberspace is an electronic realm that is theoretically unrestricted by physical limits like space or time. Some examples of cyberspace include Google and Yahoo, as well as any online areas that utilize the Internet, fixed and mobile communication networks, the World Wide Web, and all widely used social media and other applications.

Social media is an instrument that makes it easier for people to communicate with one another and with society at large in ways that newspapers and television simply cannot. However, since the advent of computers and information technology, particularly that supported by artificial intelligence, it can be characterized as computer-mediated tools that enable individuals, businesses, and other organizations to produce, share, or exchange knowledge, ideas, images and, videos in online communities and networks. Social media includes activities such as social networking, such as Facebook or LinkedIn, microblogging, such as Twitter, photo and video sharing, such as Flickr and Picasa, news aggregation, such as Google Reader, social gaming, such as World of Warcraft, social search, such as Google, Bing, or Ask.com, and instant messaging, such as WhatsApp, Google Talk, Skype, or Yahoo! Messenger.

Online service providers are those businesses that offer online services to customers online. For instance, e-transactions, medical data, social sites, Wikipedia, news sources (press), entertainment sources (music, movies), email providers, etc.

Personal data: Any fact that relates to a recognizable living person is referred to as personal data. Or any fact that can be used in conjunction with others to identify a specific person. As an illustration, consider the following: a person's name, signature, photograph, email address, identification card number, financial information, medical history, biological information, etc. Any fact relating to a named individual is considered personal data under GDPR (data subject).

Data Privacy: An individual's right to data privacy is the ability to manage their personal information. One has the right to control how their data is gathered, shared, and used. It is a component of the right to privacy, and given the complexity of technology, it must be safeguarded. Data privacy is concerned with a person's expectation of privacy as well as the proper treatment of data. The security of personal data from arbitrary actions is necessary for the current technological era. Data privacy put simply, establishes who has permission to access

the data and for what purposes. The use and governance of personal data are the main areas of data privacy.

Cloud Service The technique of providing different information technology services on demand using web tools and applications is referred to as cloud service. They use the services offered by cloud providers instead of buying them, such as data storage, servers, databases, networking, and software, and they pay for what they use and when they use them. Because it enables businesses to avoid or reduce the expense and complexity associated with owning and managing their own IT infrastructure. Large data centers are integrated inside computers to meet the ever-increasing load because of the rise in e-commerce and personal transactions. These data centers combine more servers while providing infrastructures like networking and storage. The privacy, security, and confidentiality of data kept or processed by cloud service providers are now subject to several concerns.

Artificial intelligence Technology known as artificial intelligence (AI) enhances a machine's capacity to carry out jobs that humans do. The many new technologies have greatly benefited artificial intelligence. Devices like machines, Smartphone's, and other tools help. The machine can do any work thanks to the numerous pieces of data that are provided to it as input. As a result, it would be more correct to define artificial learning as the creation of a body of information or a set of techniques by machines that incorporate human intellect.

Cyber security is the practice of guarding against malicious entry into computers, servers, networks, mobile devices, electronic systems, and data. Cyber laws are created to ensure that people do not misuse cyber technology and to stop anyone from violating the rights of others online. A special set of cyber laws was developed by the government to provide users with cyber security and to track down and prevent any immoral or illegal human behavior in cyberspace. Any sort of cyber rights infringement is considered a cyberspace infraction and is prosecuted under these rules.

Intrusion in Right to Privacy: Technology makes it more difficult for the government and judiciary to control men's inappropriate behavior. Normative, social, and legal conceptions have been upended as a result of science and technology's expansion of bounds. Without computer transactions, modern existence is inconceivable and unfinished. However, these computer interfaces frequently intrude into a person's personal space. By revealing a person's personal information, they impair both their personal and public lives. This intrusion also puts the person's privacy in peril.

Cyberstalking[8]**-** "It is a technology-based attack on one person who has been expressly targeted for such an attack

[8] Alexis, Moore A, 'Cyberstalking: How to Stay Safe and Orotect Yourself Online' Association for Progressive Communication <https://www.apc.org/sites/default/files/CyberstalkingFactSheet_0.pdf> accessed 24 Dec 2023

out of retaliation, rage, or control. The victim may be subjected to harassment, ridicule, and humiliation, as well as the emptying of his financial accounts, harassment of his family, friends, and employers to isolate the victim, the use of scare tactics to instill fear, and other behaviors. This list is not complete and could grow.

Crimes like stalking, in which a person regularly or continuously engages in harassing or threatening actions toward another person through information technology. The victim experiences ongoing harassment and feels panicked, frightened, intimidated, threatened, tormented, or molested—and with good reason. Cyber stalking typically leaves no physical harm or wounds in its wake.

The victim and the stalker typically do not need to reside in the same area to commit cyberstalking. Even third parties can be encouraged to harass and/or threaten a victim by pretending to be the victim and posting inflammatory statements on message boards and in chat rooms, which prompts readers to threaten the victim directly. The publication of a person's personal information poses a threat to his or her privacy. This can be accomplished by committing numerous violations. Some of them include:

Hacking- It refers to using the internet to illegitimately access computers. Such attacks result in the theft or harm of computer-stored data. There are different types of "hackers." The people are known as "code hackers" are experts in computers and can do whatever they want with them. Computer "crackers" breach and get around any computer system. Cryptography is a specialty of "Cyber Punks." Hacking is a threat that has grown so out of control that even the biggest businesses struggle to handle it. While the hacker may not have done anything wrong at the time, he copied the data they had access to and uses it later.

A **packet sniffer** is a software program that uses a network adapter card in promiscuous mode to capture all network packets delivered across a local area network. This mode causes the network adapter card to transfer all packets received on the physical network wire to the application for processing. Nowadays, there are numerous shareware and freeware packet sniffers accessible. These packet sniffers give users access to important and private data like account names and passwords. Many individuals use the same password to log into all their accounts and applications. Applying a single password makes it simple for network sniffers to log into the accounts and collect sensitive data.

Spoofing Attack- IP (Internet Protocol) -The act of passing off a message as coming from a reputable, well-known source is known as a spoofing attack.[9]" It happens when an attacker from outside the network impersonates a trusted machine by utilizing either an IP address that falls within the network's allowed IP address range or, an

[9] 'What is Spoofing?' Forcepoint <www.forcepoint.com/cyber-edu/spoofing> accessed 24 Dec 2023)

authorized external IP address that you trust and to which you want to grant access to certain network resources. A client-server application or peer-to-peer network connection can only be attacked using this form of attack if data or commands are injected into the existing data stream being sent between the two. He can receive any information that is sent to the original address if he is successful in changing the routing tables to the fake IP address, and he can respond just like any other trusted user.

Physical access- Theft of laptops is widespread. The computer or any of its parts are open to theft by anyone. However, stolen data from computers is more valuable and dangerous because it is stored there.

Identity theft- Anyone who wants to take someone else's identity may steal their personally identifiable information.[10] He then takes control of your finances or engages in criminal activity, like spamming.

Software piracy- It entails the theft and unlicensed transfer of computer programs, frequently via the internet. Pirated software frequently performs incorrectly and might be infected with malware.

Virus - A specific kind of harmful program or code was created to change how a computer functions and is intended to propagate from one machine to another[39]. They are computer programs that could steal information or harm computer software or data. Through the internet or storage media like USB drives and CD ROMs, they can infect a computer. By attaching to the host computer or computer software, computer viruses reproduce and create copies of themselves using the resources of the host machine. The virus itself is also activated or run when an infected file is activated or executed, or when a computer is launched from an infected disc. It frequently waits to infect the following software that is launched or the following disc that is accessed in computer memory. They spread from machine to machine and from program to program on computers.

Most viruses target laptops and desktops. There are numerous varieties of computer viruses. Some of them include a) File infectors, which contaminate files using games or spreadsheet programs. When a user launches an infected application, the viral code runs first and sets up shop on its own in the computer's memory, where it can then replicate itself in other applications that the user launches later. Once installed, the virus gives back control to the compromised programs, although the user is ignorant of this. b) Boot-sector viruses: these malicious programs live in a specific area of a diskette or hard drive that is read into memory and run during system startup. The program code needed to load the rest of the computer's operating system often resides in the boot sector. A boot sector virus can infect any diskette that is inserted into the drive once it has been loaded. Additionally, it damages the hard drive, causing the virus to load into memory each time the machine is rebooted. Boot viruses have a lot of power.

[10] Ben Lutkevich, 'Identity Theft' Tech Target <https://searchsecurity.techtarget.com/definition/identitytheft> Accessed 24 Dec 2023)

c) Macro viruses: These viruses infect files that are typically viewed as data rather than programmes and are not dependent on any particular operating system.

RESEARCH PROBLEM

In data protection, privacy is an inherent component that covers the collection, usage, and distribution of personal data. Invasion of privacy in cyberspace occurs when the users, shared personal information in cyberspace. Which is used by online service platforms without the consent of users. The risk of privacy breach becomes graver when specific personal information is accessed, used, resourced, refined, and manipulated. Technology advancement in data sharing and storage platforms in cyberspace especially backed by artificial intelligence. Which put social media platforms and online service provider ahead of users. In absence of an effective legal framework regarding protection from privacy, breach users are completely dependent on social media platforms and online service provider companies.

RESEARCH GAP

The various facets of privacy in life have been examined in several studies. Numerous publications have concentrated on how the country's development of the right to privacy as a basic right. An examination of the knowledge-sharing literature revealed several shortcomings, notably in India.

In the matter of Privacy changing dimensions. There hasn't been a detailed analysis of how the ambit of shared personal data in cyberspace has been increasing and changed over time in the nation or how courts and legislation have struck a balance in various situations. Whether the court's limits are applicable in the current context is debatable.

It is still important to analyze how the data protection laws in cyberspace work within the ambit of treaties and charters at the international level and to the examination of Indian laws in the context of maintaining individual personal data privacy.

The originality of the study resides in its examination of the strategy used by the Indian judiciary and legislation from 1950 to the present especially when social media, gaming, and financial online service platforms with advanced support by artificial intelligence and cloud service play a major role in modern time, the gap in the Indian personal data protection legislation may be observed. Without considering the constraints put in place by legislation to strike a balance between the right to privacy and technological advancement, the study of personal data privacy protection would fall short. The available literature reflects a lack of detailed discussion on personal data protection in social media platforms.

RESEARCH QUESTION

1. How are privacy and data protection issues evolving and what incidents raise concerns about personal data protection?
2. What advanced technologies are used by social media platforms and online service providers to share and store personal information (data) and how are they misused?
3. How effective are the existing regulatory frameworks at the Indian and international levels in protecting against personal data breaches?

RESEARCH OBJECTIVE

Taking into consideration started the research work with some of the objectives as follows.

1. To explore the need for the inception of privacy and personal data privacy and the general limitations on right to privacy.

2. To explore the need for the inception of Artificial Intelligence based advanced technologies in cyberspace, especially social media. And the instance of a privacy breach on social media platforms.

3. To explore the Judicial Response related to Privacy and Personal Data Protection in India.

4. To explore and to find out the legislative Framework of privacy and personal data protection Law in respect of the world and India.

5. To find out the technological awareness, and whether social sites are diminishing unity, integrity, and social cohesion among users, by collecting responses from the selected field area.

HYPOTHESIS

Technological advances in the field of information technology, such as the use of artificial intelligence on social media platforms and online services, have promoted the security of user data. The Personal Data Protection Bill, 2019 must establish a robust data protection system by making necessary changes and privacy protection requires a special regulatory authority that can focus Focus on protecting user data.

RESEARCH METHODOLOGY

Secondary data were obtained from works on personal data protection and privacy law from various academic libraries, including publications including articles, reviews, abstracts and articles other related to this study.Various search engines use the Internet to collect data related to this topic. Reviewing and analyzing legal documents is also necessary in India and other countries.

SIGNIFICANCE AND DELIMITATION OF RESEARCH

The Significance of the study includes determining the personal data privacy issue in cyberspace and to contribute to the existing knowledge system of the relevant area of the personal data privacy issue in India by highlighting the bottle neck existing in the judicial and legislative sphere. This research aims to analyze and raise critical issues in the development of privacy issues in Artificial intelligence-based advanced technology. Such problems have corrosive social effects and cause anxiety among people of a democratic country. The Researcher has been limiting the research on the personal data protection law and incidents of personal data theft, fraud, and misrepresentation. At this juncture, therefore, there is a significant need to address different aspects of the issue and propose proposals for the privacy of personal data protection in India.

MEANING OF THE TERM PERSONAL DATA, PRIVACY AND PROTECTION

The idea of personal data must be understood before one can comprehend what data privacy and protection represent. There are two broad categories of data:

PERSONAL DATA

Any information relating to a known or recognizable living individual is included. Or anyinformation that can be used in conjunction with others to identify a specific person. For instance, a person's name, last name, residence, email, ID card number, financial details, medical background, etc. Any information relating to a named or identifiable natural person is considered personal data under GDPR (data subject). Any individual, group, government agency, or institution could acquire personal data.

NON-PERSONAL DATA

It refers to data that cannot be used to identify a specific person. It has commercial worth, but no personal information is compromised as a result. Anonymized data, a company's email address, registration number, etc. are some instances of data that are not regarded as personal data.

DATA PRIVACY

Data privacy is the individual's right to ownership of their personal information. The right to control the gathering, sharing, and use of one's data exist. Due to the complex nature of technology growth, it is a component of the right to privacy and must be safeguarded. Data privacy concerns the individual's expectation of privacy in addition to

the proper handling of data. In the current technological era, personal data is a valuable resource that needs to be shielded against arbitrary actions. Data privacy, to put it simply, establishes who has permissionto view the data. Data privacy primarily focuses on how personal data is used and governed.

Personal data is related to the idea of data protection. It examines whether the information is handled fairly and legally. Data protection policies and practices aim to acquire and use the personal data of a person in a way that minimizes invasions of that person's privacy.It can be characterized as a formal restriction on who can access and use data. Data protection isthe process of preventing the unauthorized use of a person's personal information. It deals with how technology and data gathering, and distribution are related.

There are administrative measures involved in data protection as well as technical ones. Administrative action is used to describe its legal component. Data privacy is concerned with how personal data is used and governed, including things like having procedures in place to make sure that customer personal data is gathered, shared, and utilized appropriately. Data security is mainly concerned with preventing harmful assaults on data and the commercial exploitation of stolen data. Although security is required to secure data, it is insufficient to address privacy issues.

Data privacy is concerned with the usage and regulation of personal data, including the establishment of policies to guarantee that customer personal information is being gathered, shared, and utilized appropriately. Data security places a greater emphasis on defending data from malicious attacks and the commercial exploitation of stolen data. Security is essential for data protection, but it is insufficient to preserve privacy. Additionally, it is impossible to imposeprivacy in a system unless it is secure, while the opposite is not true. To create and put into effect clear and accurate data security and privacy policies, it is crucial to grasp the distinction between and link between data security and privacy.

INDIAN PERSPECTIVE OF RIGHT TO PRIVACY

“No study has given a clear picture of the existence of a comprehensive concept of privacy in ancient India”. One reason why India is somewhat isolated from the evolution of the privacy judiciary is that the initial impact of these new technologies is not felt as much as in other parts of the world. By the time the portable camera and telegraph first be gained be widely used in the United States and elsewhere in the world, India was still a remote colonial outpost of the British Empire. Although these new technologies eventually made their way to the Indian shores, they were not well established in the West until their impact on privacy was already well understood. As a result, when they were used in India, the laws governing them had already built protections. Most of the colonial-era laws still in use in India “like the IPC (Indian penal code) and the Indian Telegraph Act” are legal rules designed

to address privacy.[11]

A key feature of our system of governance is the extensive scrutiny and balance placed to ensure that state power is always kept in mind. Consequently, even if the state abuses its power to the detriment of individual rights, citizens always can resort to an independentjudiciary against the excesses of the state.[12]

Early chronicles of the “right to privacy in Indian law” date back to the last part of the 1800swhen a “British court” maintained the ‘privacy’ of a lady to enter her gallery unafraid of the neighbor's eye. Law has developed from that point forward and the privilege to privacy has been perused by the Supreme Court in Article 21 of our Constitution as a vital piece of individual freedom. Like most opportunities, we invest wholeheartedly in it, until a year ago our govt. disclosed to us that “privacy is certifiably not a fundamental right”.

The Supreme Court first told us in 1954 that “privacy is not a fundamental right”. In “MP. Sharma Vs. Satish Chandra case, eight-judge bench”, when dealing with the matter to lookand hold on to reports from the Dalmia Group, prevented the presence from getting the “right to privacy” as the Constitution expressed that the maker of the Constitution didn't visualize a similar essential right to privacy, as in U.S. fourth Amendment.

Following nine years, “in Khark Singh versus state of UP, under the watchful eye of a six- judge bench of the Supreme Court”, our desire for private life returned; just to be denied once more. Khark Singh, a supposed dacoit. He was liable for housekeeping and mystery burglary, night visits, intermittent requests, and movement looks were conveyed. The Supreme Court saidthere was no key “right to privacy” except for striking down an arrangement that permittednight visits for infringement of "individual freedom". The silver coating was the conflict of J Subha Rao, whom he said that even though the privilege to privacy was not announced as a principal directly by the Constitution, it was as yet a fundamental segment of individual opportunity. He proceeded to say, "... there isn't anything more inconvenient to an individual's actual prosperity and well being than a determined interruption into their privacy," he said.[37]

Twelve years later, Govind v. Madhya Pradesh. The Supreme Court, despite having a bench of three judges,

[11] Kartz v. United States [1970] 389 US 347
[12] Rahul Matthan, Privacy 3.0: Unloacking Our Data Driven Future (Harper Collins Publisher, Noida, 2018) 72.

maintained the presence of the crucial “right to privacy under Article 21”while facing similar factual metrics in the state. Not finish and can be meddled with by the method setup by law. Even though “Govind lost, privacy won interestingly”[13]

Privacy law was additionally fortified in the post-progression time. On account of the scandalous Bangalore hoodlum, "Auto Shankar" (“R Rajgopal v. State of Tamil Nadu”), “the Supreme Court found a contradiction between the freedom of the press and the right to privacy”& said it had won the latter. A few years after the PUCL case, the SC found a logical inconsistency between the "freedom of the press" and the "right to privacy" and said it had won the last mention. A couple of years after the "PUCL case", the court scrutinized the phone tapping of unmistakable law makers and requested that the public authority follow severe rules for tapping phone discussions. The arrangements under the “Telegraph Act,1885 and the Information Technology Act, G 2000”, managing the deterrent depend on the rules given “by the Supreme Court in the PUCL case”.[14] Unfortunately, “in the case of the right to privacy”, it took almost six decades for the Indian judiciary to finally come up with a comprehensive overhaul of the individual’s right to personal privacy.[15]

EMERGENCE OF ARTIFICIAL INTELLIGENCE IN SOCIAL MEDIAPLATFORMS AND BREACH

Information technology (IT) advancements have made the demands, difficulties, and workings of society around us more apparent. Despite this, they have also combined these aspects into streamlined, logical methods that are easy for anyone to use[16]. Information transparency refers to an organization's readiness to offer users services and organizational data. There is evidence to support a positive correlation between information transparency and disengagement. As a result, information transparency may be a useful tool for maintaining trust and participation online[17]. Likewise, information openness regarding user privacy could be employed as a privacy assurance technique given the numerous privacy concerns regarding online activity. Giving users access to information about their privacy voluntarily may therefore guarantee privacy[18].

[13] Ibid
[14] Ibid.
[15] Alan F. Westin, 'Social and Political Dimensions of Privacy', (2003) 59 J. SOC. ISSUES 431. <https://www.researchgate.net/publication/227608757_Social_and_Political_Dimensions_of_Privacy> accessed 31 Dec 2023
[16] Sasvari, Peter, ‘The Effects of Technology and Innovation on Society’ (2012) 5 Bahria University Journal of Information & Communication Technology 1-10. <https://arxiv.org/abs/1307.3911> accessed 01 Jan 2024
[17] Mohd Javaid, Abid Haleem, Ravi Pratap Singh, Rajiv Suman, ‘Substantial capabilities of robotics in enhancing industry 4.0 implementation’ (2021) 1 Cognitive Robotics 58-75. <https://www.sciencedirect.com/science/article/pii/S2667241321000057> accessed 01 Jan 2024
[18] Hofmann, Y.E., Sttrobel, M., ‘Transparency goes a long way: information transparency and its effect on job satisfaction and turnover intentions of the professoriate’ (2020) 90 Journal of Business Economics 713-732. < https://epub.ub.uni-muenchen.de/73196/> accessed 02 Jan 2024

Information and knowledge are the new Blood of the twenty-first century, containing important knowledge, insights, and potential, and they are now a necessary component of all data-driven organisms[19]. Information can be collected from data to create a variety of smart applications in several areas, including education[7], healthcare[8], construction, investment modeling, cybersecurity, law enforcement, and marketing. As a result, there is an urgent demand for advanced DBMS that can easily and effectively retrieve relevant patterns from data. Big data describes extraordinarily large data sets with more complex and varied structures. These characteristics frequently make it more difficult to store data, conduct analyses, use additional techniques, or extract results. The act of analyzing vast amounts of complex data to find hidden correlations or buried patterns is known as "big data analytics." But there is a glaring contradiction between the increased use of big data and the security and privacy it offers[20].

Variety refers to the different characteristics of the data. Several tactics have been developedin recent years to protect the privacy of big data. The phases of the big data life cycle—data generation, storage, and processing can be used to group these techniques. Access limitations and data falsification methods are used to protect privacy throughout the data creation phase[21].The methods used to preserve privacy during the data storage phase are primarily based on **encryption** techniques[22]. Additionally, composite **clouds** are used, with delicate data being managed on confidential clouds, to protect sensitive data[23].

Security Risks in Various Domains

Information Security: Threats can be anything that has the potential to harm, devastate, or adversely influence an object or object of interest by taking advantage of a security flaw[24]. Software-based attacks include those brought

[19] Mohammad Yamin, 'Information technologies of 21st century and their impact on the society' (2019) 11 International Journal of Information Technology pg 759-766 <https://link.springer.com/article/10.1007/s41870-019-00355-1> accessed 02 Jan 2024

[20] Farideh Hamidi, Maryam Meshkat, Maryam Rezaee, Mehdi Jafari, 'Information Technology in Education' (2011) 3 Procedia Computer Science 369-373. <https://www.sciencedirect.com/science/article/pii/S1877050910004370> accessed 02 Jan 2024

[21] Sabitha Sivan & Rajasree M S, 'Access Control Based Privacy Preserving Secure Data Sharing with Hidden Access Policies in Cloud' (2017) 75 Journal of Systems Architecture. <https://www.researchgate.net/publication/314487614_Access_Control_Based_Privacy_Preserving_Secure_Data_Sharing_with_Hidden_Access_Policies_in_Cloud> accessed 02 Jan 2024

[22] Jayashree Agarkhed, Ashalatha Ramegowda, Siddarama Patil, 'An efficient privacy preserving cryptographic approach in cloud computing' (2018) ICFNDS '18: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. <https://www.researchgate.net/publication/327333147_An_efficient_privacy_preserving_cryptographic_approach_in_cloud_computing> accessed 02 Jan 2024

[23] Nguyen Din Han, Longzhe Han, Dao Min Tuan, Hoh Peter In, Minho Jo, 'A scheme for data confidentiality in Cloud-assisted Wireless Body Area Networks' (2014) 284 Information Sciences pg 157-166. <https://www.researchgate.net/publication/273651315_A_scheme_for_data_confidentiality_in_Cloud-assisted_Wireless_Body_Area_Networks> accessed 02 Jan 2024

[24] Rudrajyoti Palit, 'Recent results from digital INGA at BARC-TIFR Pelletron Linac Facility and future plans' (2014) 83(5) Pramana Journal of Physics pg 719-728. <https://www.ias.ac.in/public/Volumes/pram/083/05/0719-0728.pdf> accessed 04 Jan 2024

on by Trojan horses, worms, and other malware. Malicious software, such as intrusive program code and other objects made specifically to damage a system, is collectively referred to as malware[67].These malicious programs arecommonly used by attackers:

Virus- By connecting viruses to the host computer's software, such as music or films, they can reproduce themselves and subsequently spread around the Internet[25].

Worms- Although worms are naturally self-replicating, they do not attach themselves to the host computer's software. If a network is available, they can move easily between computers, and while they won't cause much damage to the target machine, they may slow it down by using up hard disc space, for example.

Trojans- Trojans frequently offer backdoor access points via which harmful software or criminal persons can infiltrate your system and steal your sensitive data without your knowledge or consent. FTP Trojans, Proxy Trojans, Remote Access Trojans, etc. are a few examples.

Bots- Bots can be thought of as sophisticated worms. They are automated procedures created to communicate online without requiring human participation. Either way, they are possible. One host can be infected with a malicious bots, which will then establish a connection to the central server and issue commands to all other hosts connected to that bots net.

Adware- Although adware isn't strictly harmful, it does violate consumers' privacy. They show advertisements on a computer's desktop or within specific programs. They are bundled with free software, which serves as the primary source of income for such creators. They keep track of your preferences and present relevant adverts. Adware can monitor your system activity and potentially damage your computer if malicious code is embedded inside the software[26].

[25] Ali Fathi Ali Sawehli, 'Malicious Software and Security Programming Assignment - MSSP – APU' (2018) ResearchGate <https://www.researchgate.net/publication/337285394_Malicious_Software_and_Security_Programming_Assignment_-_MSSP_-_APU> accessed 04 Jan 2024

[26] Anurag Kumar Jaiswal, Dr. Nikhat Akhtar, Dr. Yusuf Parwej, Jai Pratap Dixit & Syed Qamar Abbas, 'A Systematic Literature Review on the Cyber Security' (2021) International Journal of Scientific Research and Management 9(12), 669-710 <https://ijsrm.net/index.php/ijsrm/article/view/3634> accessed 05 Jan 2024

Spyware-It is a program, or perhaps we should say software, that keeps track of your online activity and divulges the data to someone who might be interested. Most of the time, viruses, Trojans, and worms release spyware. Once dropped, they set up shop and keep quiet to stay undetected[27].

Ransomware-It is a sort of virus that will either encrypt your files or lock your computer, rendering it partially or completely unusable. Following that, a screen will appear requesting payment, or a ransom.

E-Commerce: E-commerce refers to the online system that facilitates the exchange of products and services via the Internet. Additionally, it refers to business-to-business exchanges, such as those between a manufacturer and a supplier or distributor. The services offered by e- commerce systems must be secure. Customers can, for instance, view bank statements, transmit money, pay with credit card payments, and more using online banking and brokerage services. There are numerous dangers, including the leakage of sensitive data, the transfer or destruction of data, the modification of data, the denial of services, and software inaccuracy.

IoT Devices: The vulnerability of an IoT device makes it the most vulnerable to attack. Before focusing on the underlying software, providers of IoT-based solutions start by solving this problem. Hardware and software vulnerabilities come in two varieties. A hardware vulnerability is challenging to find. Repairing the damage is more difficult, though. A backdoor in an algorithm that was badly developed is the source of the software vulnerability. Intruder conducts espionage on the targeted user using malicious software and cracking techniques to access sensitive data on the installed systems. With the aid of automated software, hackers attempt to guess a user's password. The software makes multiple guesses until it finds the correctpassword to grant access.

CYBER SECURITY

The IT Act of 2000 defines cyber security as the defense against unauthorized access, use, disclosure, disruption, alteration, or reveal of data, tools, computers, computer resources, communication devices, or information held there[28].It is also referred to as "Information Technology Security" or "Computer Security." Another way to think about cyber security is as a collection of rules and procedures that protect us from fraudsters, hackers, and other

[27]Andreas Jacobsson, Bengt Carlsson, Martin Boldt, 'Exploring Spyware Effects' (2010) ResearchGate. < https://www.researchgate.net/publication/30499314_Exploring_Spyware_Effects> accessed 04 Jan 2024

[28]Debarati Halder, 'Information Technology Act and Cyber Terrorism: A Critical Review' (2011) SSRN Electronic Journal. < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1964261> accessed 04 Jan 2024

online criminals[29]. It largely focuses on individuals, organizations, and technologies that help decrease vulnerability, online threats, deterrents, and online attacks and fraud. Cyber security and cybercrime are closely intertwined. Less cyber security will be in place as more cybercrimes occur. This can also be stated as: "User cyber security continues to deteriorate as the frequency of cyber security breaches rises." As a result, as cyber-attacks rise, so do many organizations' and businesses' fears, especially those handling sensitive data. Since they involve a computer and a network through the internet, cybercrimes are also known as computer-oriented crimes. Cybercrime is the term used to describe any criminal activity carried out online or on a computer, or Smartphone. In other terms, cybercrime is an illegal activity that makes use of computers, the internet, or both as a tool or a target.

Following is the various application of machine learning in cyber security:Antivirus software powered by AI Before utilizing any system, installing an antivirus is frequently advised. This is so that antivirus software may safeguard your machine by examining any newly downloaded files from the network to see if their signatures resemble any known viruses or malware. However, to stay up with all the improvements in the new viruses and malware being generated, this conventional antivirus needs to be updated frequently. In this case, machine learning can be quite helpful. Antivirus software employs machine learning to recognize viruses and malware by their unusual behavior rather than their signature. This enables it to deal with both common and well-known threats as well as fresh threats from recently created viruses or malware.

Artificial Intelligence and Data system security

The development of computer systems that can do tasks that are traditionally performed by humans is the goal of artificial intelligence. The ability to perceive sight and hearing, learn and adapt, reason, recognize patterns, and make judgments are some of this intellectual processes. ML, prediction modeling, NLP, and robotics are just a few of the technologies and approaches that fall under the general category of "AI." Three things have recently caused the area of artificial intelligence to advance quickly: better algorithms, more powerful networked computing, and the capacity to collect and store previously unheard-of amounts of data. Even though many people are unaware of it, artificial intelligence (AI) technologies are already being used in many areas of our daily life. The automated voice that answers the phone and welcomes you or the suggestion of a movie based on your interests are two examples of everyday AI technology. It's sometimes easy to forget that AI technologies like speech recognition, natural language processing, and predictive analytics are in use now that these systems have become ingrained in

[29] Anvesh Babu Vanamala, Ranjit Reddy Kolipyaka & Rohit Kalakuntla, 'Cyber Security' (2019) 10(2) HOLISTICA- Journal of Business and Public Administration 115-128. <https://www.researchgate.net/publication/335322600_Cyber_Security> accessed 06 Jan 2024

our daily lives.

There are innumerable ways in which AI may make life better for people. Among the promises made by AI are lower costs and greater effectiveness, considerable improvements in healthcare and research, improved auto safety, and general convenience. The benefits of AI, however, come with several challenges for society and the law. While it's feasible that AI could challenge conventional notions of privacy, it's also possible that it will help facilitate privacy in the future. The expanding usage of AI may need a review of the current level of privacy protection, but this does not mean that privacy will disappear or lose its significance. The framework that information privacy offers for selecting how we should responsibly use new technology is one of the most crucial components of privacy of personal information. AI's long- term success will depend on addressing privacy concerns and taking technological ethics into account. A balance between technological advancement and privacy concerns will promote the establishment of socially responsible AI that can eventually aid in the creation of public value.

TYPES OF ARTIFICIAL INTELLIGENCE : BASED ON CAPABILITY

1. Narrow AI or Weak AI: A fundamental form of artificial intelligence known as weak AI or narrow AI can carry out specific tasks intelligently. Narrow AI is the current iteration of AI. As they are only taught one task, narrow AI can only complete that task and cannot go beyond it. Itis set up to perform a certain purpose, such as playing chess or checking the weather, among others[30].

2. General AI: Machines that exhibit human intellect are known as "Strong" AI, sometimes known as artificial general intelligence. We can assert that machines with AGI can carry out any intellectual work that a human is capable of. This is the type of artificial intelligence (AI) that wesee in films like "Her" or other science fiction productions where people interact with conscious, sentient computers and operating systems that are motivated by emotion and self-awareness. Currently, this kind of intelligence only appears in studies and fiction. It does not exist in the realworld. However, it is still a highly challenging endeavor and academics from all around the world are attempting to construct such machines[31].

3. Super AI : Super AI is AI that is self-aware and has cognitive capabilities above and beyond those of humans. At this point, computers can perform any cognitively complex task that humansare capable of. Super AI is still a

[30] Anca Draghici, Caius Luminosu & Daniel Paschek, 'Automated business process management – in times of digital transformation using machine learning or artificial intelligence' (2017) ResearchGate <https://www.researchgate.net/publication/319012077_Automated_business_process_management_-_in_times_of_digital_transformation_using_machine_learning_or_artificial_intelligence> accessed 05 Jan 2024

[31] Emmanual Sirimal Silva, Hossein Hassani, Maedah Tajmajinani & Stephene Unger, 'Artificial Intelligence (AI) or Intelligence Augmentation (IA): What Is the Future?' MDPI. <https://www.researchgate.net/publication/340594734_Artificial_Intelligence_AI_or_Intelligence_Augmentation_IA_What_Is_the_Future> Accessed 07 Jan 2024

theoretical idea and creating such AI-enabled machines is a difficult challenge[32].

There are obstacles for government organizations wanting to use neural networks for decision-making because of unintended consequences caused by biases and ambiguous results. In a lot of the information privacy discourse surrounding AI, the growing power disparities between the organizations that collect data and the people who provide it have not been fully addressed. The majority of current models view data as a commodity that can be exchanged, which does not adequately account for how difficult it is for people to make judgments about their data when interacting with complex systems. This is especially true when the system fully comprehends them and has figured out how to modify their preferences through the ingestion of their data. Furthermore, a number of the adaptive algorithms used in AI changeso quickly that it is frequently difficult for their creators to properly understand the results they create. A significant chunk of AI's usefulness comes from its capacity to learn, spot patterns that are invisible to the human eye, and make predictions about people and organizations[33]. Artificial intelligence (AI) can produce data in a way that would otherwise be difficult to collect or that is not already available. This suggests that data that goes beyond what a person knowingly disclosed, in the beginning, is being obtained and used. Among other things, predictive technologies assert that inferences can be made from seemingly unrelated and harmless pieces ofdata. Modern technologies are already challenging the current duality of personal information, but AI blurs the lines so much that it is become more difficult to tell what is and is not "personal information." Because of the increasing prevalence of AI, all data produced by or pertaining to a human will likely be recognizable in the future. Determining what is or is not covered by privacylaw based on the definition of personal information in this context is unlikely to be technically orlegally viable, and it is also unlikely to be particularly helpful in safeguarding people's privacy. Many claims that the focus needs to be changed away from the binary definition of personal information if a privacy regulation is to continue protecting people's information privacy in anAI setting[34].

Transformational Influence of Artificial Intelligence on Digital Marketing

Artificial intelligence in marketing makes use of technology to enhance client experiences beginning with the first

[32] Bert Olivier, 'Artificial Intelligence (AI) and being human: What is the difference?' 49(1) Acta Academica. <https://www.researchgate.net/publication/320204926_Artificial_Intelligence_AI_and_being_human_What_is_the_difference> accessed 07 Jan 2024

[33] Mario Krenn, Lorenzo Buffoni, Bruno Coutinho, Sagi Eppel, Jacob Gates Foster, Andrew Gritsevskiy, Harlin Lee, Yichao Lu, Joao P. Moutinho, Nima Sanjabi, Rishi Sonthalia, Ngoc Mai Tran, Francisco Valente, Yangxinyu Xie, Rose Yu, Michael Kopp, 'Predicting the Future of AI with AI: High-quality link prediction in an exponentially growing knowledge network' (2022) ResearchGate <https://www.researchgate.net/publication/364126422_Predicting_the_Future_of_AI_with_AI_High-quality_link_prediction_in_an_exponentially_growing_knowledge_network> accessed 07 Jan 2024

[34] Miles Brundage, Shahar Avin….Sebestian Farquhar, 'The Malicious Use of Artificial Intelligence: Forecasting, Prevention & Mitigation' (2018) ResearchGate <https://www.researchgate.net/publication/323302750_The_Malicious_Use_of_Artificial_Intelligence_Forecasting_Prevention_and_Mitigation> accessed 07 Jan 2024

point of contact and continuing through the sale and beyond. AI technology also improves the return on investment of marketing efforts by assisting in the optimization of consumer-focused business strategies using machine learning, big data analytics, and other procedures. Digital marketing tasks that the AI can assist with include campaign optimization, studying consumer behavior, and making tailored recommendations. AI can also assist in automating processes like customer service and report generation. Machines now carry out laborious, repetitive tasks that used to consume a tremendous amount of human capital hours; web design and content development are both potential uses for AI software.AI can streamline marketing initiatives in digital marketing, reducing the chance of human error in the process. While most activities still require human inventiveness to be completed effectively, AI digital marketing systems can be utilized to produce reports that are only based on data. The use of digital marketing can significantly speed up business growth. It can bring about a lot of things in numerous ways when paired with technical elements like artificial intelligence. AI can be a terrific tool for supporting the ideal business expansion tactics, from sorting data analytics to comprehending consumer personas.

Chatbots are the application of AI that are frequently seen as the most revolutionary. Through their interactions with automated assistants like **Siri, Alexa, and Google Assistan**t, consumers are growing more acclimated to chatbots[35]. On many corporate websites, this technology is usedto respond to frequently requested queries by customers. The impact chatbot technology can have on the shopping experience is its best feature. Chatbots offer a cost-effective way to streamline operations and free up human agents to handle more complicated customer concerns that call for individualized care by automating the more fundamental customer support tasks[36]. Chatbots enable client support regardless of the time of day, as some organizations lack the staff to respond to customer inquiries promptly. Nevertheless, in the future, intelligent chatbots might be more involved in interactions with people, employing freshly generated responses that are beneficial for customer support, lead generation, and sales prospecting.

Companies are employing data scientists and programmers to work on their marketing strategies as technology enables the collection of increasingly complicated data. With the use of machine learning and big data analysis,

[35] Aniko Ekart, Diego R Faria & Jordan J Bird, 'Learning From Interaction: An Intelligent Network- Based Human Bot and Bot Bot Chat Bot System' (2018) UKCI'18 Conference <https://www.researchgate.net/publication/325803432_Learning_from_Interaction_An_Intelligent_Networked-based_Human-bot_and_Bot-bot_Chatbot_System> accessed 08 Jan 2024

[36] Grazia Vicario & Shirley Coleman, 'A Review of Data Science in Business Industry and Future View' (2019) 36(4) Applied Stochastic Models in Business and Industry <https://www.researchgate.net/publication/336877922_A_review_of_data_science_in_business_and_industry_and_a_future_view> accessed 07 Jan 2024

AI makes an enormous amount of data sets about consumer behavior and industry trends accessible[105]. To customize adverts, establish prices, and launch campaigns based on information about what specific customers have historically done and are likely to do, this technology enables the prediction of future consumer behavior. While advanced artificial intelligence's technical parts might seem intimidating, marketing software based on AI technology is surprisingly user-friendly.

In many ways, AI is changing the marketing sector.

Search Engines: The search algorithms get better all the time. AI integration into search engine technology enables past shopping history to be considered when browsing and suggests alternatives for misspelled search phrases. In terms of figuring out searcher intent, this software is becoming highly clever. Voice search technology is continuing to gain popularity and efficiency because AI language technology can understand complicated speech patterns and detect spoken inquiries.

Amplification of User experience: User-friendly websites and apps are continually enhancing the online client experience. Customers are more inclined to explore further interaction with a brand when they have a superior front-facing technological experience[37]. More user-friendly and individualized experiences can be produced by AI systems than could be achieved by conventional testing and optimization cycles by adjusting user experiences depending on interactions in real-time.

Data Analysis: The majority of organizations get a lot of data about their customers and industry, but they rarely make use of it. Large data volumes may be processed efficiently by AI, which can also spot patterns and trends. This enables the development of statistical models to forecast future consumer behavior as well as the development of business intelligence models to make use of that knowledge. AI can offer crucial insights for businesses to continuously improve and succeed in a more cutthroat commercial climate.

Artificial intelligence will quicken the pace of marketing trends and help marketers select the best techniques for better outcomes. The rate at which AI is transforming marketing is thrilling and fascinating, and it will only continue to spread widely in the future. It is something that will help the digital environment adopts new trends. Since search engine algorithms are also evolving to be more intelligent and user-centric, AI will strive to simplify the solution to challenging marketing problems.

[37] Wil Van der Aalst, 'Data Scientist: The Engineer of this Future' (2014) Enterprise Interoperability VI pg 13-26 <https://www.researchgate.net/publication/300575842_Data_Scientist_The_Engineer_of_the_Future> accessed 07 Jan 2024

Artificial Intelligence's Social Media Impact, Privacy Issues and Challenges Social Media

The exact concept of social media is unclear. The traditional definition of social media is any form of media that makes it easier for people to communicate with one another in society. However, the exposure that people receive from this medium is quite little.

However, it can now be described as computer-mediated technologies that enable individuals,businesses, and other organizations to produce, share, or exchange knowledge, ideas, images, and videos in virtual communities[38] and networks. Kaplan and Haenlein define it as "a series of internet-based apps that build on web 2.0's technological and ideological basis and that enable the creation and exchange of user-generated content. "Social networking sites are another name for social media websites. They facilitate communication between individuals and various entities. Social networking sites are described as web-based services that enable users to 1) create a public or semi-public profile within a bounded system, 2) articulate a list of other users with whom they share a connection, and 3) view and navigate their list of connections as well as those made by others within the system. The fact that social media are Web 2.0 internet-based services and applications is one of its characteristics. a) The foundation of social media is user- generated content. b) social media uses a variety of sources to communicate with a wide audience. Newspapers are one source of information for many recipients. c) Users build their own profiles for a website or app that social media companies construct and administer. d) By tying users' profiles to those of other people and/or groups, it helps the growth of online social networks. e) It enables a highly participatory platform for sharing, co-creating, discussing, and modifying user-generated material by individuals and the community.[113] f) It has a broad use thatcan be utilized regularly.

Social media encompasses a variety of activities, such as social networking on sites like Facebook or LinkedIn, micro blogging on sites like Twitter, photo and video sharing on sites like YouTube and Metacafe, news aggregation on sites like Google Reader, social gaming on sites like World of Warcraft, social search on sites like Google, Bing, or Ask.com, and instant messaging on sites like Google Talk, Skype, or Yahoo! Messenger. This is not a complete list;it is merely indicative. Social media also includes forums, business networks, enterprise social networks, product and service reviews, and social bookmarking. The most well-known social media platforms include Facebook, WhatsApp, Twitter, Instagram, Snapchat, and others.

[38] Martin Aruldoss, T. Miranda Lakshmi & V Prasanna Venkatesan, 'An Intelligence Models to Improve Business Perfomance' (2012) International Conference on Advances in Engineering, Science and Management. <https://www.researchgate.net/publication/254037313_An_analysis_on_business_intelligence_models_to_improve_business_performance> accessed 07 Jan 2024

Infrastructure for social media like Facebook, Google, Twitter, Instagram, WhatsApp, and Linkdin Snapchat uses artificial intelligence (AI) and machine learning-based tools and services to boost revenue while ensuring consumer satisfaction and handle time-consuming operations like social media administration[116]. AI enables social media platform operators to gain a thorough understanding of their users and their interests by analyzing the information they have contributed. As consumers occasionally volunteer their personal information to access services based on their likes and interests, this practice provides cybercriminals with opportunities to defend by manipulating and altering the information, which harms the user financially and psychologically[39].When employing a computer as a tool, many jobs can be executed more quickly and efficiently than when using human labour alone. Computers are utilized to significantly lessen the physical efforts of an individual due to the development of new techniques and the usage of new technology in many areas of daily life. However, they are currently also employed to replace the person in his decision-making process. Using the Internet of Things (IoT), less physical work is required. However, artificial intelligence and machine learning technologies are employed to replicate human cognitive processes involved in decision- making.

Facebook, One of the most well-known social media platforms has established an Artificial Intelligence Research Unit whose primary goal is to design an AJ system and evaluate its significance in relation to the users' level of intelligence. Facebook utilizes the Al tool Deep Test to track user comments and postings in many languages and dialects. Additionally, it makes use of chatbots in its application and facial recognition technology powered by A.I. that suggests tagsfor users.

Twitter is a social media site where users can post tweets about any topic to share their personal opinions and experiences. Twitter consistently states that the goal of his platform is to deliver the most appropriate tweets by prohibiting the dissemination of users' abusive messages, hate speech, and fake news. In several affluent countries, there are also penalties for similar tweets. Twitter tracks and analyses these tweets with the help of A.I.-based IBM Watson andNatural Language Processing programs for this purpose.

In addition to being owned by Facebook**, Instagram** is a social networking software that offers users a place to publish their own photographs and videos. It has about a billion users overall. To improve User by giving users a

[39] Elvira Ismagilova, D. Laurie Hughes…Yichuan Wang, 'Setting the Future of Digital and Social Media Marketing Research: Perspectives and Research Prepositions' (2020) 59(1) International Journal of Information Management <https://www.researchgate.net/publication/342863039_Setting_the_future_of_digital_and_social_media_marketing_research_Perspectives_and_research_propositions> accessed 07 Jan 2024

platform where they may find numerous photographs of a variety of activities, many places, several events, top restaurants' favorite foods, and varied life experiences using big data and AJ Additionally, hate speech and cyber bullying posts are found using Deep Text, and they are taken down from the website.

Whatsapp is a freeware cos platform owned by Meta Platform that allows users to exchangetext messages, photos, audio files, and videos over the internet using their Smartphones[40]. It is a reasonably priced app. The automated software Whatsapp chatbot, which is based on Al technology and Al-based Cloud services, is used by WhatsApp to store user-shared data on this platform.

The next iteration of the Internet, called the **Metaverse**[41], is all about social interaction. Users "live" within a digital realm using a combination of many technological aspects, such as virtual reality, augmented reality, and video. Science fiction author Neal Stephenson first used the word "Metaverse" in 1992, and video game firms frequently use it nowadays. The idea is gradually assuming enormous relevance since numerous tech behemoths have already started theprocess, with Facebook and Epic leading the way.

Deepfakes is another resource for bogus information. The term "Deepfake," which combines "deep learning" with "fake," refers to artificial intelligence programs that combine, replace, and superimpose photos and video to produce convincingly fake movies and images[42].Since then, numerous nations, including India, have employed deep fakes frequently in politics. Following that, a low-cost user interface for the Deepfake algorithm was made available via the Reddit app Fake App, allowing anyone to produce Deepfakes without any prior programming or machine learning experience. Later, a number of variants were created, including Face to Face App and Open Face Swap.

When we use Google or Apple Maps for navigation, when we use Uber, or when we buy an airline ticket, AI is at work. AI is a primary goal for Google, and it is used in many of its products. In the banking and financial industry, artificial intelligence

[40] Chen Yang, 'Research in the Instagram Context: Approaches and Methods' (2021) The Journal of Social Sciences Research <https://www.researchgate.net/publication/349117428_Research_in_the_Instagram_Context_Approaches_and_Methods> accessed 12 Jan 2024

[41] Deepti Kelkeri, Prahalad Tadasad & Shobha Patil, 'Usage of WhatsApp Messenger amongst post-graduate students in a University environment: A Study of Karnataka State Women's University, Vijayapura' (2015) 2 International Journal of Multidisciplinary Research and Development pg 591-594 <https://www.researchgate.net/publication/294557467_Usage_of_WhatsApp_Messenger_amongst_post-graduate_students_in_a_University_environment_A_Study_of_Karnataka_State_Women's_University_Vijayapura> accessed 12 Jan 2024

[42] Cuong M. Nguyen, Duc Thanh Nguyen, Thanh Thi Nguyen...Viet Quoc Pham, 'Deep Learning for Deepfakes Creation and Detection: A Survey' (2019) ResearchGate <https://www.researchgate.net/publication/336055871_Deep_Learning_for_Deepfakes_Creation_and_Detection_A_Survey> accessed 12 Jan 2024

is widely used for projects like fraud detection, chatbots, and investment. In our daily lives, artificial intelligence has assumed a prominent role. AI has a tremendous impact on how we live because technology is used in so many facets of daily life.

Judicial Decisions on Right to Privacy and Data Protection in India

Though before independence, some decisions were given by the Supreme Court ofundivided India, in which the Right to Privacy was upheld. In India, the vacuum of absence of common law provisions for protection of privacy is filled with the judicial activism of Supreme Court. The Supreme Court of India has come to rescue of common citizen by construing 'Right to Privacy' as a part of fundamental right to life and personal liberty under Art. 21 of Constitution of India.

As in other judicial systems, the right was associated with enjoyment of property in India,may it be house or land. As India was ruled by England, we can see the development from the 19th Century. The courts in British-India upheld the right in different cases. These decisions were given by British India Courts and the Judges of Sardar Diwani Adalats.

After Independence

Under Indian Constitution, there is no specific enactment for Right to Privacy as such andalso there was no legislation for protection of privacy. Therefore the invasion on the right by was challenged on the ground of invasion on right to life and liberty i.e. Art. 21. Various contours of right to life and liberty including right to privacy are explored by the courts. Courts, in many cases touched the various aspects of right to privacy, i.e. against property for search and seizure to disclosure of information and upheld this right under the fundamental right governed under Article 21 i.e. Right to Life and several other provisions of the Constitution read with the Directive Principles of the State Policy.

In Context of Personal Liberty

Right to privacy was judged in the context of personal liberty of the person and decision was given by Supreme Court in following case. Right to Privacy was not well-known till the decision in Kharak Singh was pronounced by the Hon'ble Supreme Court. This was decided for the first time in Kharak Sing's case and the first tort explained by Prosser i.e. intrusion upon person's solitude was upheld by Hon'ble Supreme Court.

In **Kharak Singh (1963)**[43], the Police Regulations in UP were challenged. The petitioner was challenged in dacoity but released as there was no evidence against him. The police opened history sheet against him. Definition of history sheets was provided in Regulation 228 of ChapterXX of U. P. Police Regulations as personal records of criminals under surveillance. He was put under police surveillance. Under the Regulation 236 of Police Regulation UP, Surveillance involves—a. Secret picketing of house or approaches to the houses of suspects, b. domiciliary visits at night, c. periodical enquiries by officers not below the rank of sub-inspector into the repute, habits, association, income, expenses or occupation, d. the reporting by constables and chaukidars of movements, absence from the house, e. the verification of movements and absence by means of inquiry sips and also f. collection and record on sheet of all information bearing on conduct[44].

The Petitioner challenged the constitutionality of Chapter XX of UP Police Regulation and in particular Regulation 236. It was also contended by the petitioner that surveillance, and untimely visits of police breached his right to privacy. The case was decided by six judge bench.

In majority judgement, the U.P. Police Regulation was held valid. The petitioner challenged thathis right to privacy is violated by late night knock on his door.

When this case was decided, the principles governing the inter-relationship between the rights protected by Art. 19 and the right to life and personal liberty under Art. 21 were governed by the judgement in Gopalan case as it considered the right protected under each article as distinct right and not overlapping. The majority judges held because of picketing, the freedom to move freely, guaranteed by Art. 19 (1) (d) was not infringed[18]. It was held that, Art. 21 is not applicable in this situation as right to privacy is not guaranteed in our constitution. So if the police is only ascertaining the movements of the person, it is one of the method, and so is not breach of fundamental right under the constitution[45]. So in Kharak singh also court held that rightto move freely under Art. 19 (d) is distinct right and has no relation with right to life under Art. 21.

But domiciliary visits under S. 236 (b) was held invalid as against the right to life protected under Art. 21. Court held that, the word ‘personal liberty’ shall not be construed to exclude the invasion and intrusion in man’s personal security as his right to sleep is a necessity for his existence even as an animal. The court held that in Preamble the words ‘dignity of individual’ are used and protection of it ensures the full development of a person. The court held that the words personal liberty shall be construed in a reasonable manner and in the same sense which would

[43] Kharak Singh v State of Uttar Pradesh AIR 1963 SC 1295.
[44] U.P Police Regulation and Police Act, 1861.
[45] Kharak Sing v. State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR(1) 332, para 340

promote and achieve those objectives.[46] It was held by majority that right to life is infringed by the domiciliary visits at night. But the decision was not based on right to privacy.

But in minority judgment given by Subba Rao and Shah JJ that out of other surveillances, surveillance by domiciliary visit was held against the person's right to privacy under Article 21. The Hon'ble Judges held in minority that by untimely visits, even in night to the house of a person breaches his right to privacy. While discussing the restraints on free movements, the courtheld that restraints can also be created by certain conditions apart from scientific methods. It washeld that personal liberty lies in freedom from encroachment on the personal life of any person and not only from the freedom of movement. The court also reiterates that right to privacy is essential part of personal liberty even though it is not declared specifically by the Constitution.

The court explained that person's own home is very sacred place which provides him rest, physical happiness and security and peace. It is his 'castle'. His home, where he lives with his family, protects his privacy from encroachment by society. The court has stated that what is opined by Frankfurter J., in Wolf v. Colorado [(1949) 238 US 25] about importance of security of one's privacy against arbitrary intrusion by the police, is also applicable to Indian home. The Court held that physical encroachments on his private life would affect it in a larger degree than the physical restraints on his movements. Interference with the privacy is harmful for his health. Therefore it was held that, "We would, therefore, define the right of personal liberty in Art. 21 asa right of an individual to be free from restrictions or encroachments on his person, whether those restrictions or encroachments are directly imposed or indirectly brought about by calculated measures. If so understood, all the acts of surveillance under Regulation 236 infringe the fundamental right of the petitioner under Art. 21 of the constitutions."[47]

First time it was discussed that whether Right to Privacy could be implied from existing fundamental rights. In a limited way, Hon'ble Supreme Court recognised that Right to Privacy exists and included in Art. 21-Life and liberty of the person. The ratio of Kharak Singh ruled the scenario for more than ten years till in Govind's case Supreme Court held in favour of the right.

In **Govind (1975)[48]**, the Supreme Court assessed more elaborately the right to privacy. The petitioner has challenged the Madhya Pradesh Police Regulation-855 and 856 made under s. 46 (2) (c) of M.P. Police Act, 1961. The constitutional validity of regulation which provides surveillance was challenged. Regulation 855 provides that on information, if the District Superintendent believes that a particular individual is leading a life of crime and the

[46] Kharak Sing v. State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR (1) 332p. 351
[47] Kharak Sing v. State of Uttar Pradesh AIR 1963 SC 1295, 1964 SCR(1) 332 p.358-359
[48] Govind v. State of Madhya Pradesh AIR 1975 SC 1378

behaviour ofthat individual show determination to lead a life of crime, that individual's name may be ordered to be entered in the surveillance register and she would be placed under regular surveillance. Regulation 856 provides that such surveillance may consists of domiciliary visits both by day and night at frequent but irregular interval. The said Regulation was challenged on two grounds, a. Regulation is not framed under s. 46 (2) (c) of Police Act, 1961 and have force of law, b. even if they are framed under section 46(2) (c) of Police Act, 1961, provisions regarding domiciliary visits offended Art. 19 (1) (d) and Art. 21.

The court upheld the regulation. It was ruled that regulation is 'procedure established by law',and therefore it is not violating the Art. 21. The Court had observed that Constitution makers were aware of the values propounded by Brandeis J in Olmstead29 relating to spiritual nature, feelings and his intellect. They were also aware about the pain, pleasure and satisfaction from theuse of material things. To protect these spheres from the government actions, they have conferred certain space where he should be let alone.[49]

The court accepted the fundamental right to privacy in limited scope emanated from Art. 19(1) (a), (d) and 21. It was also held that this right is not absolute and reasonable restrictions can be placed thereon in public interest under Art. 19(5). The fundamental right can be overridden by the compelling state interest. It was held, "There can be no doubt that privacy- dignity claims deserve to be examined with care and to be denied only when an important countervailing interest is shown to be superior. If the Court does find that a claimed right is entitled to protection as a fundamental privacy right, a law infringing it must satisfy the compelling state interest test. Then the question would be whether a state interest is of such paramount importance as would justify an infringement of the right."[24]Court had considered the decisions given in cases of Wolf v. Colorado and Griswold along with the European Convention regarding Right to Privacy. Mathew, J, observed that "Assuming that the fundamental rights explicitly guaranteed to a citizen have penumbral zones and that the right of privacy is itself a Fundamental Right, the fundamental right must be subject to restriction on the basis of compelling public interest."[50] The court denied the claim of the petitioner.

In changed political scenario, to collect the information about the political rival, tapping of the telephone of him was practiced widely. The same action was practiced by police to gather evidence also. Action of the state by tapping of the means of communication, telephone at that time, was under scrutiny that whether such action implies to invasion of privacy of an individual.

[49] Govind v. State of Madhya Pradesh AIR 1975 SC 1378. P.155
[50] Gobind v. State of Madhya Pradesh AIR 1975 SC 1378

In **R. M. Malkani (1973)[51],** where the police officer, during investigation of case, with the authority of petitioner, attached the tape recorder to his telephone and obtained the evidence of illegal gratification. It was contended by the petitioner inter alia that the evidence of telephonic conversation is obtained illegally in contravention of S. 25 of Indian Telegraph Act and therefore inadmissible as evidence. S. 25 provides that if a person intending to intercept or acquaint himself with contents of any message damages, removes, tampers with or touches any battery, machinery, telegraph line, post or other things whatever, being part of or used in or aboutany telegraph or in working. It is punished with imprisonment or with fine or with both. The Court observed that the tape recorder was attached to the telephone with authority of the petitioner and therefore there is no breach of the provisions of S. 25 of Indian Telegraph Act and evidence obtained is admissible. The petition was dismissed but Supreme Court stated that telephonic conversation of an innocent person would be protected by the courts against wrongful or high-handed interference by tapping of the telephone conversation by the police. Though it was not linked to right to privacy but the protection was given on the same line as tapping of the telephone is also considered as breach of privacy.

This aspect of privacy, is a personal communication, and by intrusion and invasion on itis by tapping of the telephone was covered under PUCL's case in detail. Earlier the same issue was discussed in R. M Malkani but as the tapping was done with the permission of the owner, the protection was denied. The question whether tapping of telephone is constitutional was discussed in detail in the case of **People's Union for Civil Liberties (1997)[52]**. Telephone tapping is permissible in India under S. 5(2) of the Telegraph Act, 1885. The writ petition was filed by voluntary organisation due to mass tapping of the telephones under S. 5(2) of Telegraph Act, 1885 and challenged the constitutional validity of the same.

In Context of Freedom of Speech and Expression and IT Act, 2000

The case which has challenged the fundamental right under Art. 19 (1) (a) and not fundamental right under Art. 21 is the case of **Shreya Singhal[53](2015).** Two ladies commented on Facebook, a social media site, about the total closure of Mumbai City after the death of influential political leader. The police arrested both of them under S. 295A of Indian Penal Code and under S. 66A of Information Technology Act, 2000. They were released afterwards and also the cases were dropped which were filed against them. Under S. 66A of Information Technology Act, 2000, law enforcement agencies can arrest and prosecute the person without warrants on thecharges. The action raised alarm in the minds of people.

The women filed a petition challenging the constitutional validity of S. 66A of Information Technology Act, 2000

[51] R.M.Malkani v. State of Maharashtra AIR 1973SC 157

[52] People's Union for Civil Liberties v. Union of India AIR 1997 SC 568, (1997) 1 SCC 301

[53] Shreya Singhal v. Union of India, AIR 2015 SC 1523

on the ground that it is infringing the fundamental right granted under Art. 19 (1) (a), freedom of speech and expression. The only restriction on the right is provided under Art. 19(2). They argued that provisions under S. 66A are very vague to restrict the right to comment on the internet which is covered under right under Art. 19 (1) (a).

Under S. 66 A of IT Act, 2000, if any person who sends message through electronic communication which contain any information which is grossly offensive or of menacing character or the information which he knows it is false but sends it to cause annoyance, inconvenience, danger obstruction, insult, injury, criminal intimidation, enmity etc. or sent for purpose of causing annoyance or inconvenience etc. is guilty. The petitioner contended that the parameters which is restricting the person's right to expression by sending messages using electronic media are vague. Such parameters shall be in consonance with parameters provided under Ar. 19 (2). The government contended mere chance of abuse of the provision may not be aground to declare the provision unconstitutional. Legislature is best position to fulfil the needs ofthe people. Also loose language of the provision cannot be the ground for invalidity because law is concerned with the novel ways to disturb rights of the people through internet. So if the statute otherwise is legislatively competent and non-arbitrary it is valid and cannot be declared unconstitutional.

The Supreme Court held that S. 66 A of IT Act, 2000 is capable of all types ofcommunications on internet. The Court found that it does not make any distinction between mereexpression of opinion or discussion and the message which cause annoyance to somebody. Thelaw fails to establish the close relationship with the intention to protect public order. The Courtfurther held that commission of an offence is complete after sending the message. It does notdistinguish between the sending it to one person and sending it to masses to create public unrest. The Court held that government failed to show that provisions under S. 66A are for theprotection against communication inciting the commission of an offence. The Court observedthat acts pertaining to mere causing annoyance, inconvenience, danger obstruction, insult, injury,criminal intimidation, enmity etc. or merely grossly offensive are not the offences under IndianPenal Code.

For the contention of the petitioner that the provision is vague, the Court verified the United States cases and held that, "the statute which does not lay down reasonable standards for defining guilt in a Section which creates offence and which does not provide any guidance for law abiding citizens or authorities and courts, Section which creates the offence and which is vague shall be struck down". The Court was of the opinion that S. 66A leaves many terms vague and undefined and therefore is not valid. Court observed that by providing for annoyance or inconvenience, it restricts many innocent speeches. The court declared in unconstitutional.

Importance of the case is that that it is deciding the rights of the parties relating to freedom of speech and

expression. The court narrowed down the exercise of power under such vague provisions fixing the liability on the persons.

J. K.S. Puttaswamy (Retd.) challenged this collection of personal information under Aadhaar scheme. Many cases have filed in the courts all over India challenging this collection byState.

Whether 'Right to Privacy' is to be considered as fundamental right or not, this question arose again when constitutional validity of Aadhaar framework (uniform biometric based identity card) which government wanted to make mandatory for receiving government services and benefits. It was challenged before three judge bench of Supreme Court by retired High CourtJudge, **J. K.S Puttaswamy[54] (2012)**. In this petition the collection and use of biometric and demographic information of an individual under Aadhaar scheme was challenged. It was contended that it is violating the fundamental Right to Privacy and therefore invalid. Supreme Court was asked to decide the validity of Aadhaar Act. The Advocate General of India argued that even though many Supreme Court judgements upheld the right to privacy, but Part III of Constitution does not guarantee this right specifically and separately. Moreover, the larger Supreme Court benches in M. P. Sharma (8 judge bench) and Kharak Singh (6 Judge Bench) alsorefused to decide in favour of Right to Privacy. As a result of this, the court referred this case to larger bench consisting five judges to ensure "institutional integrity and judicial discipline".

Again on 18 July, 2017, the constitutional bench presided over by Chief Justice of India was of the opinion that this constitutional question shall be placed before larger bench consisting nine judges to decide the status of Right to Privacy authoritatively. The petitioner argued that Right to Privacy is an independent right included under right to life (with dignity) and personal liberty under Art. 21. The Respondent argued that Constitution provides protection for personal liberties which incorporate Right to Privacy in a limited sense.

The bench consisted Kehar C. J, Agrawal J, Nazeer J, Chandrachud J, Nariman J, Bobde J, Kaul J. Sapre J and Chelameswar J. The judgement of 547 pages contains six opinions and many observations. Justice Chandrachud wrote plurality judgement for four judges (Kehar J, Agrawal J, Nazeer J, and himself). Nariman J, Bobde J, Kaul J, Sapre J and Chelameswar J each wrote separate concurring opinion. The main issue before the court was whether Constitution of India protects Right to Privacy.

Information Technology Act, 2000

The Information Technology Act, 2000 was enacted with the objective of providing legal framework for facilitating e-commerce, e-governance and protecting privacy of individuals. After enactment of the Act, information and

[54] J. K. S. Puttaswamy & Anr. V. Union of India & Ors. W.P (Civil) 494 of 2012

communication technology through internet has engulfed almost all human activities at alarming speed. Almost all transactions of businesses and also the governments were done through internet. Due to its omnipotent and omnipresent nature, security, confidentiality and privacy was threatened. There were only two options, either to enact new legislation covering the protection of transactions done through information and communication technology via internet or amend or modify the existing legal provisions under Act.

Indian Government has chosen the second option of amending the IT Act, 2000. Thegovernment selected to amend and enact some more provisions in the existing Act instead of enacting new legislation for data protection. This Act was amended in 2008 and its scope iswidened. It covers many new activities including provisions for data protection and crimes.

Information Technology (PSIMADI) Rules, 2009

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 were passed to provide control. It provides the procedure to conduct interception. However, the privacy of individuals is considered, as it is provided that such interception requires prior approval from the competent authority, i.e. the Secretary in the Ministry of Home Affairs in the case of the Central Government and the Secretary in charge of the Home Department in the case of the State Government. In an emergency, a separate method must be followed.. The purpose for interception must be the same which is specified in S. 69(1) of Information Technology Act, 2000, i.e. for protection of sovereignty and integrity of India. It is mandatory to record reasons for Interception. Interceptionis permitted for the period of 60 days and on renewal not to exceed 180 days.

Intercepted communications shall be kept confidential not only by intermediaries but their employees. Rule 25 forbids its disclosure except to an official of an authorised agency who may use such information only for specific purposes as directed by competent authorities.[55] Rule 23 prescribes that unless the intercepted information is required by law, it should be destroyed after six months. The power of interception is regulated with the provision that competent authority shall first verify whether there are alternative means to acquire the information. If it is observed that such alternative mean or method is not available then and then only the direction for interception, monitoring or decryption is issued. Government's power to intercept or monitor or decrypt without finding other means to get information is checked and regulated by this and interests of individuals are protected.

[55] IT (Procedure and Safeguard interception, Monitoring and Decryption of Information) Rules, 2009, Rule, 25

After interception, monitoring and decryption, the data is collected and used by the government. There are two actions, one is interception, monitoring and decryption of information and other is monitoring and collection of traffic data or information. For collectionof traffic data, interception is essential. For these two actions different legislations are enacted.

CONCLUSION

The internet, particularly social media, provides a unique avenue for the exchange of distinct ideas, goods and services as well as information. The benefits of these technology cannot be disputed. Technology innovation and excessive, unprotected utilisation of it, however, have the potential to hurt users more severely. In modern digital culture, any information about a person can be transformed into information that can be used to identify him. When privacy is violated or invaded due to the processing of personal data by anyone, including the government, the general public turns to the courts for protection.

Hence, in present research work, study was focused on the concept of (personal information) personal data protection with reference to privacy and Personal Data Protection Act , regulations, and rules. This research was done with following objectives-

1. To explore the need to inception of privacy and personal data privacy and the general limitations on right to privacy.
2. To explore the need to inception of Computing advance technology like artificial intelligence in cyber space specially social media. And the instance of privacy breach at social media platforms.
3. To explore the Judicial Response related to Privacy and Personal Data Protection in India .
4. To find out the technological awareness, and whether social sites are diminishing unity, integrity and social cohesion among users, by collecting responses from selected field area.

The study was separated into five chapters in order to accomplish the aforementioned study objectives. All the objective of study have been addressed. In addition to identifying the objectives and developing the hypothesis, the researcher does a thorough literature study in the first chapter of the introduction.

SUGGESTIONS

1. India should create a robust data protection law to protect personal data privacy, similar to other developed nations like the European Union, the United States of America, and the United Kingdom.
2. Additionally, the government must be held accountable for breaches in data security and privacy. The government is given various exemptions under the Personal Data Protection Bill of 2019 in relation to its operations.
3. It is necessary to clearly address cloud service providers' liability. The intermediaries and service providers must be held strictly liable. The obligation of cloud service providers must be made clear.
4. The terms imposing liability must not be vague or confusing when defining liability.
5. Provisions governing the government's ability to gather data from intermediaries andservice providers

must be implemented in a specified manner.

6. Control and rules for the installation and usage of CCTV and biometric data gathering equipment should be specified.
7. There is an urgent need to pass a comprehensive Privacy Act. The government should form an expert group to investigate incidents of privacy violations and adopt legislation only dealing with such issues. Our government should undertake a public consultation to determine how to improve data protection and privacy safeguards. "The proposed Privacy Act will harmonise, rather than homogenise."The Act should consists enforceable provisions of right to privacy for netizens/citizens, provisions ofdynamic grievance redresser mechanism, well defining a deterrence structure in case of noncompliance of rule and regulations, must included a comprehensive effective monitoring mechanism, a suitable and well-explained provision to reduce overlap with other laws
8. The law governing data protection must advance along with technology. It should contain exceptions, but they should be strictly outlined and constrained. The law shouldn't be under pressure as a result of the exceptions. "Any restrictions on the right to privacy should be in accordance with the laws now in effect and should only cover those aspects that are required in a democratic state," says the Constitution.
9. Encryption defends against "other attacks," "stealing of data," and "invasion ofprivacy" for Internet users. “Therefore, the most appropriate and secure method for End-to-end encryption can be achieved by the sender encrypting the communication before it leaves his computer rather than relying on a corporation or firm to accomplish it.. If the data is intercepted, only the hyper text will be visible.
10. To maintain the open internet, international protections and harmonisation must be implemented. It indicates whether there is a good law. It should be modified and used as inspiration to apply them here. For instance, under the GDPR in Europe, every time you open a website, the website must ask you if they can track you or not.You have the option to accept or reject. India was the first country to adopt it. Additionally, we will make it clear what information will be tracked and let you decide if you wish to accept it or not.
11. For authorities to gather, use, monitor, and store information, the government should establish explicit procedures. India does not currently have enough privacy protections in place for cases where the government conducts surveillance. Inadequate privacy protection is provided by the current system, which is focused onnational security.
12. The use of policies, user agreements, and other terms and conditions must be made clear to end users, and language used should be as simple as feasible. Users should sign agreements that are clear and concise. In order to effectively use data, the user must first be made aware of its origins and intended applications. Consequently, before using or storing data, informed consent is required. Despite declining to sharehis data, the user still needs authorization to access some websites or resources.
13. A breach of privacy should not just be the responsibility of State actors but also of non-state actors.

Legislators need to act right away to safeguard and strengthen the right to privacy as a separate right.

14. Government surveillance ought to be kept to a minimum. The government must realise that privacy is not about keeping information secret; rather, it is about having the freedom from unauthorised interference.
15. The management of other government programmes and the distribution of subsidies should be handled by programmes like Aadhaar, but they shouldn't turn the system into a surveillance State. To reduce identity theft and prevent other types of forgeries, Aadhaar's security and privacy protections should be strengthened.
16. Strict penalties for privacy violations should be included in the law, but for the time being, it is important to ensure that the law does not unnecessarily hamper practical technological advancements.

In broader sense every individuals should be made their self aware of privacy problems while using any social media platform, mobile app, commercial site as overhalf of the country's population has access to the internet. We had nearly 700 million internet users in last year's, and that number is expected to increase to million or may be more by 2025. It is imperative that individuals become informed and well aware with data breaches and how they affect their rights.

Meanwhile, privacy jurisprudence remains a source of worry across the world. Individual independence and liberty have been pushed for by the rise of liberal democracy and the internationalization of human rights. And technical advancements in IT(specially artificial intelligence), particularly in the fields of media, communication platforms in cyber space, have had an major influence on privacy issues. Debates regarding the nature of privacy will intensify, making the subject an interesting issue to research. Privacy is conceivable in the digital era which is developing into virtual reality ;all we need is the confidence that it is possible. It is a work in progress, and there is still more to be done.

BIBLIOGRAPHY

Books / Acts / Rules

1. Bakshi P.M , "Hand book of Cyber & E- Commerce".
2. Gill S.S, " Information revolution in India- A Critique".
3. Dudheja V.D "Crimes in Cyber space(Scams & Frauds)".
4. Sawhney Ashok Air Cmdre (Retd.) The Emerging Security Challenges(2010).
5. Dr. Gupta and Agrawal, "Cyber Laws" first edition 2008.
6. Matthan, Rahul, "Privacy, 3.0, Unlocking our Data driven Future", Harper CollinsPublishers India. (2018)

7. Chaubey Dr.R.K, "An Introduction to Cyber Crime & Cyber law", Edi 2008.

8. Sharma Vakul, "Information Technology Law and Practice", 2ndEdition.

9. Tayal Dr.V ,"Privacy in Indian technology regime–Issues and challenges"

10. Mali Adv. Prashant, "Cyber Law and Cyber Crimes", 2nd Edition,2015,

11. Vivek Sood, "Cyber Law Simplified", Twelfth Reprint 2013, ISBN-10:0-07- 043506-5.

12. Dwivedi Yogesh K, Mishra Santosh K & Huges Laurie," Artificial Intelligence: Challenges and opportunities for India",Yojan magazine, Jan2020.

Websites

- http://www.itsecurity.gov.in/ - Official site of Security site on Info Tech in India.
- http://www.ncrbindia.org/ - Official site of National Crime Records Bureau.
- http://en.wikipedia.org/wiki/Data_Protection_Act
- http://www.niscair.res.in/ScienceCommunication/ResearchJoumals/rejour.
- www.cybercrime.in
- www.cyberlaws.net/cyberindia/cybercrime.html
- www.techterms.com/definition/cybercrime
- www.usdoj .gov/criminal/cybercrime/reporting.htm.