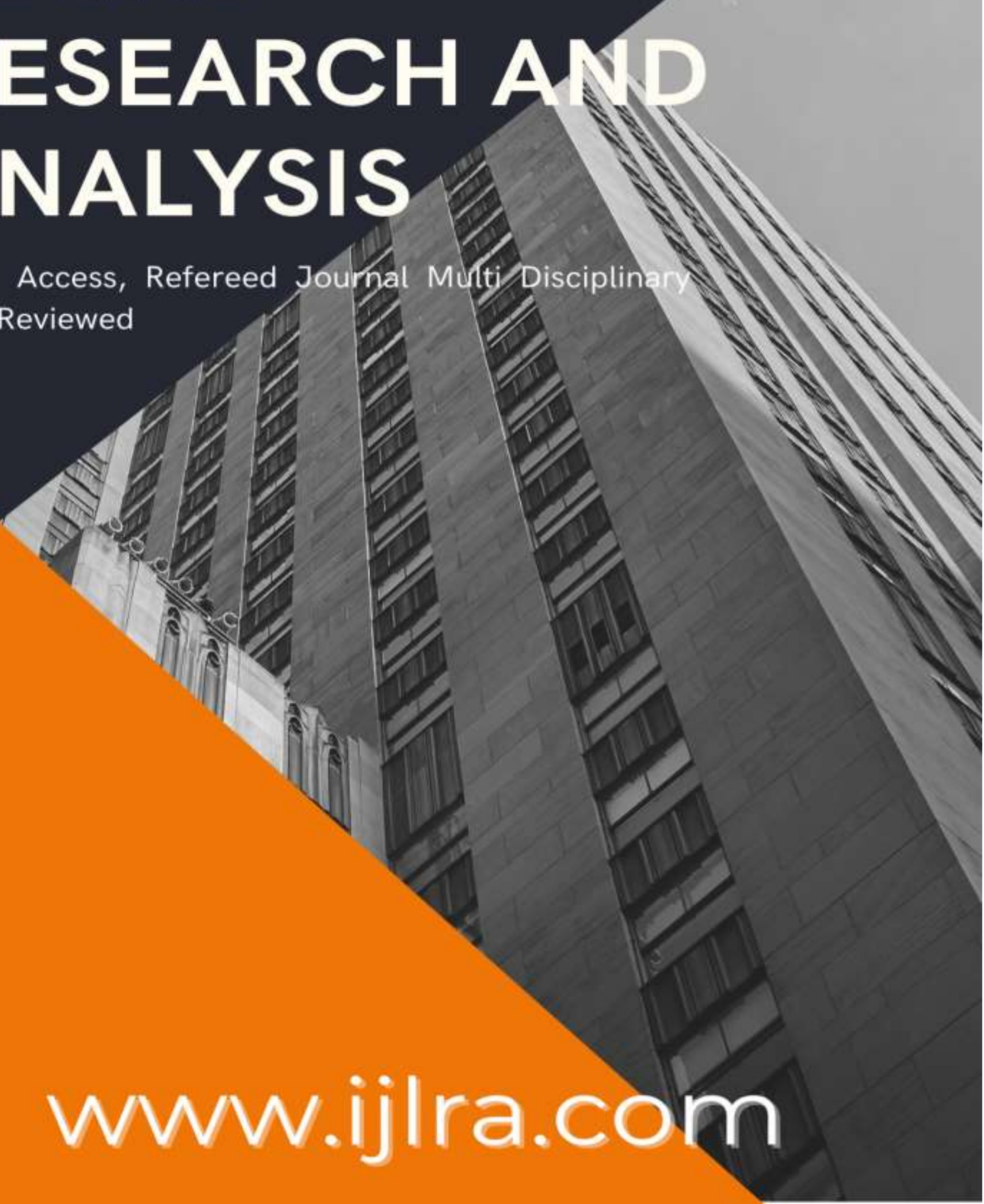
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.
Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

INDIA'S DATA PRIVACY IMPERATIVE: BRIDGING THE LEGISLATIVE GAP IN THE DIGITAL AGE

AUTHORED BY - ABHISHEK SINGH[1] & DR. SANJAY KULSHRESHTHA[2]

Abstract

This paper deals with issues related to data privacy. The protection of data has turned out to be an enormous threat to developed or developing economies around the world. This research aims to understand three different dimensions, which include legal, technical & political.

Technology plays a vital role in globalization and with the increase in communication, people are sharing personal information on the internet. "Data is the new oil," which is evident from the conduct of tech giants such as Facebook, Google, Amazon, Microsoft, etc.

Data is playing a major role in the 21st century, and a smartphone has become an integral part of our lives; whether knowingly or unknowingly, Users are constantly sharing a lot of personal information through their electronic gadgets, such as photos, location, political interests, bank details, debit cards, preferences, travel history, behavior, etc. With the growing use of AI applications, even minute information from an individual plays an important role.

The growing concern alarmed the developed countries like the UK, which have already prepared the legal framework for data protection, so they have to implement DPA (Data Protection Act, 1998), and the USA implemented ECPA (Electronic Communications Privacy Act, 1986), but India does not have specific legislation dedicated primarily to maintaining privacy and data protection for its citizens. Although the Supreme Court of India brought the right to privacy under the ambit of Article 21 of the Constitution of India, we are in dire need of legislation to protect the privacy of every citizen of this country, and the current IT Act, 2008, was not enacted with the intent to protect privacy.

The purpose of this research is to identify the problem and to find a comprehensive solution for the legal framework concerning data protection and safeguarding privacy.

[1] Phd Research Scholar, School of Studies in Law,. Jjiwaji University
[2] Professor, Dean, School of Studies in Law, Jiwaji University

Keywords:* *Data, Privacy, Technology, Legislation, India.

INTRODUCTION

The Internet is the biggest invention of the 21st century and is constantly developing. Today, we are living in an era of information where users are constantly getting themselves updated through social media, news, and other applications.

It can be observed that, after the smartphone came into existence, there is a rapid growth of the internet; in India itself, according to recent stats, about 700 million people are connected to the internet. Prime Minister Shri Narendra Modi asserted a focus on digitalization and launched a campaign called Digital India. The initiative was launched to connect every individual in our country with the internet so that citizens can seek any information about the schemes introduced by the government and can benefit from them. The Digital India initiative was launched with the primary focus of connecting all the villages of the country with internet services in order to improve its infrastructure, universal digital literacy, and deliver government services digitally.

In the last decade, it can be observed that smartphones as a commodity have become accessible and are being used by billions of people around the world. People are exchanging their ideas through the internet, education, social media, online marketing, etc. After the COVID-19 pandemic, the internet turned out to be a quintessential necessity for every individual as work from home and online meetings on Zoom and Microsoft Teams became an essential part of human lives. Even education is being imparted through online classes.

Like the physical universe, we have a data universe, which is doubling in size every two years, and by 2020, we will reach 44 trillion Gigabytes. An enormous amount of data is being shared by the individual every second; some information is shared knowingly, and a lot of data is shared inadvertently, which is a matter of concern. Artificial intelligence is c

It cannot be denied that in today's globalizing world, the internet has turned out to be the biggest facilitator and connected billions of people throughout the world, but surely, with every benefit, there is a dark side to the "age of information." In this digital age, '*if you're not paying for the product, then you are the product.'* The data we have been sharing, whether knowingly or unknowingly, we don't know what is done with the data that is collected.

ISSN: 2582-6433

It is often said that "we are living in the age of information." The bigger question is, "Are we really living in the age of information or misinformation"? As we all must have observed personally, how easily fake news is circulated through social media platforms, minds are getting polarised by the kind of social media posts we see on these platforms, manipulation techniques performed through these social media platforms, and when you look around you see the world is going crazy.

Giant tech corporations like Google, Facebook, Twitter, etc. are rendering their services for free to their users, they never charged people for being on Facebook, using the google android platform, or Twitter, but they are constantly feeding on that data provided by you, which helps them monetize and currently these are leading corporations with a revenue of billions of dollar every year.

Every single second is spent by the user on the social media website, and internet search engines feed on the data provided by the user. Further, raw data is collected by the system and harvested. Hence, it allows them to predict user behavior, which helps them to monetize through advertisements.

Now the question is, how secure is our data? In our daily lives, we tend to share a lot of sensitive information on the internet without being concerned, about whether the sensitive data is shared by us like credit card numbers, bank account details, ID cards, PAN numbers, UID numbers, biometric data, preferences, behavior, pictures, patterns, etc. every single piece of data which is collected, is it secure?

There are various forms of technologies that are introduced, which are getting updated every single day to make the personal experience of a user better than ever, which is posing an imminent threat to the privacy of an individual.

Thus, a serious need for attention to be paid to the data protection bill in order to protect the privacy of the citizens of India, because currently, India does not have any legislation with respect to maintaining the privacy of an individual and data protection. Although we do have the Information and Technology Act, 2000 but the scope for data protection in it is quite narrow.

Since data protection is a primary concern for the developed nations, and in order to maintain it, the UK brought legislation for data protection based on the OECD guidelines Data Protection Act 1998 was enacted in the UK. Whereas in the US, Congress is concerned about privacy and introduced the US privacy act in 1974, and later the Electronic Communications Privacy Act, 1984 was enacted.

GLOBAL DATA FRAMEWORKS: HISTORICAL CONTEXT

The US government at the beginning of 1970 observed that there is an automated system that stores information about individual that can be a threat to their privacy. An advisory committee was set up by the government known as the Department of Health, Education, and Welfare (HEW). The HEW committee had to identify various legal and technical issues with respect to the rapid increase in data processing. The committee submitted its report titled '*Report of the Secretary's Advisory Committee on Automated Personal Data System'*. The recommendations of this landmark report suggested by the committee, the US Congress developed a code of fair information practices based on the fair information practices principle (FIPPS). The code specifies how data should be stored, managed, handled, and maintains the privacy and security of the individual.

The code of FIPPS became the basis of the laws for the protection of data around the world. The Organisation for Economic Co-operation and Development privacy guidelines followed the lead of FIPPS, and the committee of OECD committee initiated preparing the legal framework for data protection around the world. The OECD guidelines inspired several nations and organizations to adapt and prepare the legal framework for the enactment of legislation for data protection in their respective country. The UK government enacted the Data Protection Act, 1998(DPA); similarly, Australia prepared Australia's Privacy Act, 1988, and Japan introduced the Protection of Personal Information Act, 2003.

The expeditious advancement of the technology is turning this legislation ineffective, and thus OECD issued new guidelines in 2013, which were heavily criticized by the member nations because it did not suggest reasonable methods for a new technology known as big data.

III. INDIA'S PRIVACY JURISPRUDENCE

A. CONCEPTUAL FOUNDATIONS OF PRIVACY

The word 'Privacy' is derived from the Latin word "privatus," which means "separate from the rest." The word *'Privacy,'* according to Merriam-Webster dictionary, means *'freedom from unauthorized intrusion.'* With the advancement of technology, it has become a challenge for an individual to keep their data private.

The conceptual foundations of privacy are anchored in its philosophical evolution, legal recognition, and socio-technical dimensions. Philosophically, privacy traces to Warren and Brandeis' seminal 1890 articulation of the "right to be let alone," framing it as protection against invasive publicity and emerging technologies like instant photography.[1] This conception evolved through Kantian dignity theory, where privacy enables moral autonomy by shielding intimate decisions from external coercion.[2] Contemporary scholar Helen Nissenbaum reframed privacy through *contextual integrity* – arguing violations occur when information flows breach situation-specific norms (e.g., health data shared with employers).[3]

Legally, privacy manifests as:

- Informational control (Westin's definition of regulating personal data disclosure),[4]
- Spatial non-intrusion (prohibiting physical trespass like *Kharak Singh*'s nocturnal surveillance),[5] and
- Decisional autonomy (Cohen's model of freedom from algorithmic manipulation in personal choices).[6]

The digital age has further fragmented privacy into technical sub-concepts: confidentiality (data encryption),[7] anonymity (unlinkable identities),[8] and agency (user sovereignty over profiling).[9] These layers converge in critiques like Zuboff's "surveillance capitalism," exposing how tech giants commodify behavioral data, transforming privacy from a right into a market externality.[10]

B. CONSTITUTIONAL EVOLUTION THROUGH CASE LAW

The Supreme Court of India, in its landmark judgment in *K.S. Puttaswamy V. Union of India*, where a former Justice of the High Court, Shri K.S. Puttaswamy, filed a petition before the Supreme Court challenging the government Aadhar scheme, where the government was collecting biometric data (fingerprints, iris scan) and providing a unique identification code to its citizens. Also, the Aadhar card needs to be linked mandatorily with bank accounts, PAN, etc., to reap the benefits of the social schemes introduced by the government.

The petitioner challenged the constitutional validity of Aadhaar and contended that the scheme is violating the privacy rights of the citizens. The respondent argued that the constitution of India, in *M.P. Sharma case, a constitutional bench of 8 judges, decided that the constitution of India does not guarantee the 'right to privacy as a fundamental right of the citizen.*

The nine-judge constitutional bench gave its verdict and overruled the decision given in the landmark case of *Kharak Singh vs. the State of UP (1961),* where it was held by the supreme court that "*the expression 'life' was not limited to bodily restraint or confinement to prison only but something more than mere animal existence*," the domiciliary visits at night by the UP police were considered as the invasion of personal liberty, although the apex court didn't expressly state its decision concerning privacy the essence of the right of privacy can be inferred from its decision.

The nine-judge constitutional bench unanimously decided that Article 21 of the Constitution does guarantee the 'right to privacy as a fundamental right, overruling the judgment given in the MP Sharma vs. Satish Chandra and Kharak Singh vs the State of U.P.

C. POST PUTTASWAMY LEGISLATIVE INITIATIVES

The government of India, after the Supreme Court judgment, formed a committee of experts headed by former Supreme Court Justice B.N. Srikrishna in order to understand issues related to data protection in India. This committee is formed to study and prepare a legal framework for the laws relating to data protection in the Indian sphere. For a developing economy like India, the legal framework should not act as an obstacle for the entrepreneur, and on the other hand, the privacy of the user should not be affected. In the modern era, with the advancement of technology.

The white paper has been drafted by the members of the committee, keeping in mind the difficulties faced by other countries, their experiences, and the grievances they dealt with them. The draft of the 'white paper is published in the public domain and available on the Ministry of Technology & Information website, and even the general public is allowed to read the draft prepared by the committee and leave their suggestion and feedback.

IV. TECHNOLOGICAL THREATS TO PRIVACY

There are various technologies that have been introduced to improve the personalized experience for a user. In this section, I'll discuss the challenges pertaining to the drafting of a data protection bill with growing and advanced methods that are designed by companies to collect the personal data of a user.

A. SOCIAL MEDIA & PERSUASIVE TECHNOLOGY

There are 2.45 billion Facebook users around the world, and in India, there are 290 million people using Facebook. People often think that they are socializing and connecting with their friends and family through these platforms without any cost, but it's way more complex than that. "When you're not paying for the product, then you are the product." Companies like Facebook and Google work on improving user experience. According to the *definition given by ISO, "user experience includes the user's preferences, beliefs, behavior, psychological responses, perceptions, and emotion that occur before, during, and after use."* Social media companies like Facebook, Twitter, Instagram, and Snapchat work on three simple goals, i.e.

Engagement goal: the team of experts and AI tools that try to make the user engaged with the screen for a longer time. The more time a user spends on the screen, the more data is extracted by the companies. Every single action of the user is closely monitored, for example, what image you look at and for how long you look at the image, every second counts—the people's engagement to their screen by keeping them scrolling. The collection of data that is procured gives them a great amount of certainty, which helps them to predict the user behavior, which helps them monetize their business and advertisers are willing to pay for such services, where there is a guarantee that if the advertisement places it will be successful. The tech industry is making its approach toward engagement goals and developing addictive behavior for its users to keep them engaged; no wonder these companies are billion-dollar companies.

Growth goal: They want users to help them grow and spread it across their friends and family to join and create a bigger user base, which helps them procure more data.

Advertisement goal: this is how these companies monetize as they feed on the data provided by the user, which helps them recognize a pattern and behavior which helps them make room for the advertisement. They can persuade a user to buy a product online,, which is why all the companies prefer this platform to advertise.

ISSN: 2582-6433

PERSUASIVE TECHNOLOGY

A technology that is designed to persuade the user by influencing them through social media. The user data is collected by his behavior and preferences and the kind of posts he likes and shares on the social media page, and on the basis of that data, similar posts and advertisements are suggested through the algorithms. This technology is generally used in politics, sales, religion, etc. This technique is manipulative in nature, which arouses the user to build a perception in their mind. The idea is to persuade the users and keep them hooked their screens. Every second spent by the user on their screens

FACEBOOK- CAMBRIDGE ANALYTICA DATA LEAK

In 2018, the world came across the biggest data leak scandal in the history of Facebook. In this case, it was claimed that Facebook allegedly leaked the data of millions of Facebook users, and without the user's permission, that data was harvested by a British company called Cambridge Analytica, which was a British political consulting company that helps political parties to influence their voters. Cambridge Analytica collected users' data from 2013 in an application where a series of questions were asked & collected personal data of the user without their knowledge, which helped them create a psychological profile of the user. Cambridge Analytica sold the user data for political campaigns in the US presidential election. The information about the breach was disclosed by an employee of Cambridge Analytica, Christopher Wylie, who revealed it in an interview by the Guardian and telegraph.
Facebook was fined by the UK commissioner for leaking the personal data of its users, which is violating the right to their privacy.

Even now, Facebook keeps conducting different experiments, and they keep rolling out tiny experiments on its users to understand their patterns and behavior better. A/B testing is one such tool through which they understand the user's pattern, so A/B testing helps them understand the words, phrases, videos, testimonials, etc.—creating such words that directly land you on the page and grab the attention of the visitor. These are all persuasive technologies, and these social media companies feed on the data, which helps them monetize their business in a big way.

DATA MINING & ARTIFICIAL INTELLIGENCE

A process through which usable data of a user is extracted, which is further processed by the businesses so that they learn more about the patterns and behavior of their customers. This helps them anticipate the most probable outcome for the customer who visits the website. Whenever the customer is online shopping, we often share personal information unintendedly about our consumption, behavior, and pattern with the retailer. That behavior is studied, which helps them predict the commodities that the customer might find useful in the future.

Similarly, a case took place in the state of Minnesota, the USA, where a giant retail company, Target, through this data mining technique, figured out a teen's pregnancy. They allot every customer a guest ID card, and it contains the history of all the products that were bought or checked by the customers along with their phone numbers and email ID. In this particular case, Target through data mining technology sent the high school teen coupons suggesting she buy baby products. When the father came to know about those emails to his daughter, he went to the Target store and complained about it; later, it was found out that his teen was actually pregnant, and Target was right about the pregnancy. This sounds eerily creepy how much they can figure out about us through the data they acquire from us.

Massive scale contagion experiment: The mental and emotional state of a person can be triggered through social networks. The user's mental state can be easily manipulated and triggered by what he perceives from social networking. For example, there are two users, and who search for a topic on Wikipedia; it will give them the same result, despite their choices and preferences. Whereas, when you are on social media, they know about the pages or kind of posts you prefer, so for every set of users, there is different information, unlike Wikipedia. Different emotional states (depression, happiness, sad, anger) can be triggered through the social network, and it can be observed by the marginal gap by making people more polarized towards political parties. All these emotions are triggered without the user's awareness by collecting his personal data. Serious manipulative techniques are being used by these giant social media companies by feeding on their data and monetizing through advertisement.

Artificial Intelligence: The origin of artificial intelligence can be traced back to world war 2, where Alan Turing gave the concept "can machines think?''. Developing a machine that is intelligent and through the data which is provided to it, a preferred outcome can be realized by the machine is artificial intelligence. During world war II, the mathematician Alan Turing helped allied forces breaking the nazi encryption machine, also known as the "enigma" this groundbreaking discovery of machine learning became a winning model for the allied forces against the Nazi army.

Today this tool can be used to make people more addicted to their screen, and the tech giants can create the desired outcome by feeding on personal data by invading their privacy. One of the examples is the youtube recommended video tool, which can keep us engaged on the screen for longer than usual. These algorithms also create a series of recommended videos that are aligned with the user's personal ideology. For example, If you're searching for a conspiracy theory that the 'earth is flat,' these algorithms can suggest a series of videos that can make you believe by showing different videos.

That's how fake news travels six times faster, and people have observed violent action because of the fake news.

III. LEGAL CHALLNEGES

The Internet is considered the biggest invention of the 21st century, and the exponential growth of the tech industry in terms of money and user base can be observed.
"*Uber, the world's largest taxi company, owns no vehicle. 'Facebook', the world's most popular media owner, creates no content. 'Alibaba' most valuable retailer has no inventory, and 'Airbnb' world's largest accommodation provider has no real estate"*.
These are the most profitable and revenue-generating companies, minting billions of dollars every year. Although all these companies have created a lot of jobs and made our lives convenient like we can hire a taxi from anywhere, book a hotel, transfer money through our bank account, do online shopping, and connect with people through social media. Have you ever thought about how much personal data is shared by the user? A lot of times, we tend to share sensitive information whilst signing up on these applications.

A sensitive piece of information shared by the user like PAN, Aadhar, credit card number, bank details, biometrics, location, Email ID, contact number, address, etc. is the data that is shared by the user. There is other information that is also shared, of which the user is unaware. All this data procured can seriously affect our privacy rights, and currently, India has not made any specific legislation to maintain a user's privacy.

A. Current Legal Framework of India

At the moment India does not have any legal framework specifically for Data protection. Currently, there are certain frameworks that provide relief but not adequate protection for the privacy control mechanism. As of now, we have Article 21 of the constitution, Information and Technology Act, 2000, Indian telegraph act, Indian penal code, and Indian contract act. But these legal frameworks are insufficient and do not provide rules relating to the storing, processing, and protection of private sensitive information. There is no specific procedure for the storage, transmission, and methods of safety to secure personal data, in fact, data is not restricted within the certain territory of India, and particular legislation is required for the cross-border flow of it.

However, The information and technology ACT, 2000 amended, and sections 43A and 72A were added, where section ***43A states that "Compensation for failure to protect data. - Where a body corporate, possessing, dealing, or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected".***

Section 72 A prescribes punishment for disclosure of information in breach of lawful contract and for the breach of such private personal information, imprisonment up to three years with a fine which can be extended up to 5 Lakh Rupees.

Suggestions:

Data protection was not the primary intent when the Information and technology act, of 2000 was enacted, as the scope of data protection in the act is inadequate. IT act, 2000 has a very limited scope with respect to protection for the private personal information of the user and provides no agency of the government to regulate it.

The state of California became the first state in the united state of America to enact the California consumer privacy act which came into force on 1st January 2020. The recent development of such an act can be an inspiration for the rest of the United States of America and us.

The committee led by retired justice Srikrishna has already submitted its report with respect to the data protection bill and is under consideration and hopefully, it will cover all the aspects regarding data protection of the citizen. Data is playing a prominent role in this era and acts as a sufficient threat to the country.

Conclusion

As we are moving ahead in the age of digitalization. There is a specific need for strict legislation with respect to the data privacy act. As we have recently observed, India banned 117 Chinese applications under section 69A of the Information technology act. These Chinese apps were also an emergent threat with the risk of violating the privacy of its user and the threat was critical enough that the ministry had to ban such apps as they were posing a threat to the sovereignty of India.

We have also observed in our daily lives that we keep receiving unintended calls from the bank and other companies, surprisingly they have ample information about us. Strangely we never pay much attention to it. Even shopping apps like amazon, youtube, google, etc. keep on suggesting things that we need, even if you haven't searched for it. Well, there is definitely a breach in our privacy and currently with this progressive technology.

References:

1) White paper on data protection framework. https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf
2) Ministry of information and technologyhttps://www.meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited
3) Indian Constitutional Law(7th edition), MP Jain.
4) The constitutional law of India (49th edition), JN Pandey
5) KS Puttaswamy vs union of India https://indiankanoon.org/doc/127517806/
6) Experimental evidence of massive-scale emotional contagion through social media.https://www.pnas.org/content/111/24/8788
7) Target baby 360 cases. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#3d811b506668
8) Artificial intelligence. https://builtin.com/artificial-intelligence
9) https://www.prsindia.org/theprsblog/background-section-66a-it-act-2000