Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 4 Issue 3 (2024)

Privacy in the Age of Artificial Intelligence: Addressing the Ethical and Legal Implications

Maria Devi Angerhofer[1], Dr. Samrat Datta[2], Anil Kumar Vishwakarma[3], Udit Raj Sharma[4], Dr. Vinita Singh[5] & Pooja Gautam[6]

Abstract

The modern technology can be called the byproduct of the second world war. Ever since then there has been a drastic change in the way we humans live and our interdependence on the use of technology. AI (Artificial Intelligence) has helped in drastically advancing various sectors for instance healthcare, enforcement of law, social media and engineering. At present we are in an era in which can get information about just anything and anyone. Unknowingly our photos and details can be seen and missed used just by anyone. Apart from it your conversation can also be overheard by the technologies present in your room. That is why we observe some people sticking tape on the screen and mic area. Another such instance we can observe is that some parents avoid posting photos of their children on social media platforms and stop others from doing so. Such concerns have become very relevant. As apart from the good side that AI has contributed to in our human lives. There is a very dark and scary side as well. It has caused an increasing concern that AI is eroding our traditional concept of the right to privacy. In this paper we will examine the conflict between the right to privacy of an individual and the use of AI. Especially keeping in mind, the AI technologies which are particularly dealing with data collection, surveillance and decision making and their challenges with the traditional notion of privacy. It will be vocal for enhancing privacy protection in the regime of AI. By emphasizing the need for robust regulatory measures and increasing transparency and the development of a more ethical AI practice. It has been accepted that AI has become an integral part of our life's, and we need to find out a feasible solution in which right privacy and AI can co-exist, by analyzing the existing legal framework including the General Data Protection Regulation (GDPR). This article will identify the regulatory gaps that failed miserably to address the emerging privacy issue. This paper underscores the importance and need to keep a balance between technological innovations on one hand and safeguarding the fundamental right of privacy.

Keywords: Artificial Intelligence, Right to Privacy, Fundamental Right

1.1 Introduction

The digital advancement we are enjoying today goes way back approximately 200 years. It was in 1830, when Charles Babbage invented 'analytical engine.' It was the first of its kind, which could process and store information consisting of multiple purposes and flexible configuration of usage. Alan Turning, another scientist invented the 'turning machine' in 1936 which could make calculations of large information. It also played a major role in the Second World War. The major technological advancement took place between the period of the Second World War and the Cold War, which drove nation to spend more on the invention of technologies.[7] Eventually giving rise to what we call today as AI (Artificial Intelligence). AI can be defined as a concept that is used to give meaning to a set of computer system, which is able to learn analysis and respond from their own experience and therefore also able to solve complex problems.[8] For instance, Vacuum cleaner or Washing Machine early they were just tools that help us in households and couldn't function without our command. Now we have AI based Vacuum cleaner who move around the house and keep on cleaning once they sense dirt. On the other hand, we have washing machines which have an in-built system and it will independently function on its own without our need to be there and continuously give commands. Similarly, matching of prices and vehicles while renting and Uber. AI also collects and demonstrates the user what he likes to see on social media platform, such information is collected by

[1] Assistant Professor, School of Law, UPES, Dehradun Uttarakhand, India.
[2] Assistant Professor (SG), School of Law, UPES, Dehradun Uttarakhand, India.
[3] Assistant Professor (SG), School of Law, UPES, Dehradun Uttarakhand, India.
[4] Assistant Professor (SG), School of Law, UPES, Dehradun Uttarakhand, India.
[5] Professor, School of Law, UPES, Dehradun Uttarakhand, India.
[6] Assistant Professor (SG) School of Law, UPES, Dehradun Uttarakhand, India.
[7] Adrian Athique, *Digital Media and Society: An Introduction* (Polity Press 2013).
[8] Akshita Jain, *AI: A Threat to Privacy?* 1 Indian J.L. & Legal Res. 1 (2021).

either listening the conversation of the user by checking past records.[9] These were some basic examples of impact of AI in our daily lives. AI also has a drastic impact on various sectors across the world. Like the Global Economy, the Banking system and our Health Care.

Across the world AI has drastically impacted our Economy. Traditionally we used to go to shops and buy the desired product. However, with the help of AI any person sitting in any part of the world can go online to select a product and order it. Similarly, there are various other impact which are as follows:

i. **Digital Platform and Expansion of Business:** The nature of business establishment and its expansion has become extremely easy on the one hand and the competition has also increased rapidly on the other. For Instance, 97% of small businesses in America, who have established their online platform like Amazon and E-bay and export through their AI platform export their products to other countries. Whereas only 4 percent of companies who do not use an AI platform export their products.[10]

ii. **Language Barrier is no longer a Barrier:** Earlier it was exceedingly difficult to expand a business in different countries. Since language was one of the major barriers. However, with AI as a platform it has become extremely easy to translate and remove such barrier[11].

iii. **Automating Routine Task:** With the expansion of business there come higher responsibility in maintaining the stability in the market. Therefore, the owners would be rather more concerned with respect to the higher level of duties. AI would automate these processes, and it would also help in being a time safer.[12]

iv. **Increase in Efficiency and Accuracy:** Under the traditional method of handling complicated task like pay roll or enrolling workers in health insurance programs. There were chances of error, which caused chaos as it lead to delays and inaccurate payments. However, AI would remove such errors and therefore increase the efficiency.[13]

As observed from the above, AI has a significant impact on the global market and its economy. By 2030, with the help of AI there would be a global boost of 14 percent of the GDP.[14]

Apart from the impact on the global market AI has also played a drastic change in our Banking System. It has been observed that the traditional form of human centric to a computer and data driven financial industry has been rapidly increased in sector of financial technologies (FinTech).[15] Apart from the FinTech re-evolution has also developed in financial section in other areas as well, which are as follows:

1. Compliance.
2. Fraud and anti-money laundering (AML) detection.
3. Lending and credit assessments.
4. Cybersecurity.

---

[9] The Evolution of Artificial Intelligence: Past, Present & Future, *Analytics Insight* (July 4, 2024), https://www.analyticsinsight.net/artificial-intelligence/the-evolution-of-artificial-intelligence-past-present-future.

[10] Dhananjai Rana, *The Impact of AI on Global Expansion*, 4 Indian J.L. & Legal Res. 1 (2022-2023)
[11] *Ibid*
[12] *Ibid*
[13] *Ibid*
[14] *Ibid*
[15] Jon Truby, Rafael Brown & Andrew Dahdal, *Baking on AI: Mandating a Proactive Approach to AI Regulation in the Financial Sector*, 14 Law & Fin. Mkt. Rev. 110 (2020).

5. Trading and investment decisions.[16]

Moreover, AI hasn't only brought a boom in the commercial sector, but it also has played a vital role in the Legal Profession as well. As one of the major issues faced in the legal profession is backlogging of case. However, long prolonged cases ultimately delaying justice which is a violation of the principle of fair trial based on the phrase 'Justice delayed is justice denied.' With the implementation of AI, there has been a change in the amount of time a case requires to be solved. Drafting and producing evidence has become much easier. In the present day across the world many courts and law firms have and are under the process of updating their offices with technological advancements. The vision is that in the near future artificial intelligence (AI) will have authority to monitor and take decisions about petty crimes and civil dispute. As a result, Judges would be relived of such cases, they can concentrate on more important matters which requires human intelligence.[17]

From all the development that is done in terms of AI is that in the end of the day everything is accumulated in the form data. Data which will hold very important and confidential information which may be very sensitive like the data of a country or data which will totally infringe a human's privacy. In this article our major concern would be that how to safe our human right of privacy with the present development in AI.

1.2 Background

Artificial intelligence is a field of computer science, which deals with creating programs that can perform tasks that are performed by human intelligence. As a result, the task performed by the computerized machine can be performed with intelligence and it will include visual- audio perception. The capability of it will also learn and adopt to commands, provide reasoning and help in decision making of the human being.[18]

With the breakthrough of Artificial Intelligence is made to stay on one hand but on the other hand it has raised various concerns in respect to unparalleled challenges that will arise in securing the fundamental right of privacy.[19] Fundamental rights are considered basic right that is availed to the citizens of a country. These rights are granted to them because they are human beings and without them no human being can function to their best credibility and living would become impossible. Fundamental rights are one of the core pillars of a democratic country. In the universal aspect given a border inspiration of fundamental rights are derived from Human right[20]. The researcher would like to state that the principal idea of human rights and fundamental right is based on one stone, which is the stone of some sort of regulated freedom granted by the ruling State.

Right to privacy is a universally recognized fundamental right.[21] It an essential right as it encompasses the individual's right to keep any information, activity and communication which is preserved as personal, to remain protected and private from any unauthorized intrusion. For instance, I might like roaming at places and not what it be saved by google that I visited that place. Privacy is perceived to be linked with personal autonomy, which is related to capacity to make decisions

---

[16] A. Baker, R.S. Eisner, J.M. Pennell & E.A. Raymond, *Investing in AI Fintech Companies*, in *Artificial Intelligence & Financial Services* (Mayer Brown Spring 2019), available at https://www.mayerbrown.com/-media/files/perspectives-events/events/2019/04/article-booklet.pdf.

[17] Sai Dheeraj Dronadul & D. Vijaya Bhaskar, *Impact of Artificial Intelligence (AI) on Legal Profession and Justice System*, 6 Int'l J.L. Mgmt. & Human. 1084 (2023).

[18]Artificial Intelligence and Privacy – Issues and Challenges, *Office of the Victorian Information Commissioner* (July 16, 2024), https://ovic.vic.gov.au/privacy/resources-for-organisations/artificial-intelligence-and-privacy-issues-and-challenges/..

[19] *Ibid*

[20] Wenxian Zhang, *Human Rights Jurisprudence in the New Era*, 18 J. Hum. Rts. 265 (2019).

[21] In the United Kingdom, the right to privacy was recognized in *Campbell v. MGN Ltd*, [2004] 2 AC 457 (HL). In the United States, the right to privacy was established in *Griswold v. Connecticut*, 381 U.S. 479 (1965). In Austria, the right to privacy was enshrined in the Austrian Constitutional Court ruling *G 147/86* (1988). In India, the right to privacy was affirmed in *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, (2017) 10 SCC 1.

in one's own life without intrusion or interference. The pillar support under right to privacy is to protect people's honor and safety.[22]

The importance of right to privacy is to protect the reputation of people and protect people falling prey to undue scrutiny judgment and stigma. Ultimately, enabling them to speak openly and freely without continual fear of exposure or intrusion. Right to privacy acts like cloths. Since mental safety and physical safety are directly linked to the ability to maintain privacy. There might be an argument that the right to privacy can be an hinderance in finding criminals and prosecuting them. What if it is the other way round, meaning to state that the right to privacy helps to protect individuals from harassment, violence and any other changes. Moreover, it make it harder for criminals to steal other people identities, by keeping their information like medical and finance, personal address hidden. Moreover, if the government helps it citizen to keep their information safe and confidential a trust bound relation arises between the citizens and state, which is essential for both ends.[23]

It is here that the concern arises that in modern era with the rapid development of AI that the state is curling away our right to privacy on one hand and that people are exposed to fall prey in being exposed. These technology relies upon vast amount of data, data which is being saved somewhere. The concern that arises is that how this personal data is collected processed and used? It presumed that that this data can be missed used.[24]

The researcher would like to give a very simple example like for instance: some have uploaded a photo on status on Facebook, WhatsApp Instagram or any other social media platform. Some one sitting miles away not knowing you can use that child's photo and with the help of AI change that photo into a lady of 30 years and create a fake identity and use it to make crime. Now the fear in the common society is to what extend can it lead? What will be the consequences? The above example was a very simple example. There are various other examples. Some of the key risks which are associated with AI and privacy are as follow:

a. Possibility of breach: Artificial intelligence works like our human brain. The human brain is based on memory; accordingly, they act. Artificial intelligence on the other stores this memory in the name of data, which is required for training and decision-making. The concern is that many a times this data contain very sensitive data, which is personal. For example, information relating to someone's health, financial transaction, biometric identities like fingerprint retina etc. If no proper care is taken in handling this data, there can be a possibility that such data may fall into the hands of unauthorized entities, leading to possibility of misuse such data, ultimately causing violation of one's privacy.
b. Possibility of Bias and Discrimination: The algorithmic used by artificial intelligence is very direct, it will only be concerned whether the given task is meeting the requirement or not. As there is lack of emotional intelligence like human beings do. It cannot think holistically that is why chances will arise of bias and discrimination and unfair outcomes especially in sensitive matters like hiring, lending and enforcement of law.
c. Tracking and surveillance: Artificial intelligence has made it very easy for anyone to track a person. They use tools like facial recognition, location tracking. It raises concern of mass surveillance and infringement of an individual's privacy, leading to erosion of privacy and civil liberties. It has created a sense of fear like in George Orwell's famous book called '1984'.[25]
d. Vulnerability in securing data: At present artificial intelligence is vulnerable to attacks like breach of data, adversarial. It can be exploited to large extend as it can be subject to stealing and manipulation of sensitive data.

[22] Supra note 10.
[23] Jessica G. Mecellem, *Human Rights Trials in an Era of Democratic Stagnation: The Case of Turkey*, 43 Law & Soc. Inquiry 119 (2018).
[24] Ujwala Uppaluri & Varsha Shivanagowda, *Preserving Constitutive Values in the Modern Panopticon: The Case for Legislating toward a Privacy Right in India*, 5 NUJS L. Rev. 21 (2012).
[25] George Orwell, *1984* (Secker & Warburg 1949).

AI, driven decisions or compromise the integrity and reliability of the system and therefore it poses a significant risk to privacy and security.[26]

1.3 AI Technologies and Privacy Concerns

The objective of AI was to mimic the intellectual intelligence of a human being. Technically, it is a computer that tries to learn the process of reasoning and solving of problems similarly to the capacity of a human being. In this process a lot of information need to be feed to the AI (computer), in the form of data. As a result, the AI will become a trained model, which will use the data as a reference.[27] Each time an AI runs around of data processing it will measure its performance and develop accordingly. So that each time it will be more expertise in its task. AI being a machine never needs a break, it can perform vast amount of task without any break and the rate of performance is also very quick as compared to our human contra part. In a broad understanding of how AI works? Is that AI isn't just a single set of computer programs, but it is a complete set entire discipline of science. It's ultimate goal is to create a computer system, which is capable of being a replica of a human in terms of behavior and thinking processes. To solve complex work and problems in a very short span of time. [28]

From the above the researcher would like to explain it in a very simple language. Artificial intelligence is nothing but a part of science which deals with computer regulated programs. It is a complex system of program and wiring, through which a machine gets life. With this help information in the name data is fed into it so that it functions as desired. After the information is feed the machine will start to function like a human being, by performing complex task in a very short span of time, however not only the amount the time needed to complete a task is short but also the amount of work done in a very short period of time is equally bigger as compared to the our human counterpart.

One such example is AI chatbot which is feed with information like text that can learn to generate and create lifelike that would be an interface between the machine and human. Acts like image recognition can be learned, which will help in describing objects. In the back end this done by reviewing millions of images that are feed in. [29]

There are various stages allocated in it, which is as follow:

i. Machine Learning: In building a system of AI, it must go through a process called 'machine learning'. In it the computer must learn from a larger database, it is done by way of identifying relationships and patterns from the data. It uses statistical technique, which will help it to learn progressively better at a task without it being specially programmed for the certain task. It is a method in which historical data is used as an input to predict the new outcome. It consists of two methods. On one side it 'supervised learning' here the expected output is already calculated and known with the help of labeled set of data. On the other hand, is the 'unsupervised learning' since there is no labeled set of data therefore the expected set of data is unknown.
ii. Neutral Networks: The researcher would like to call it rewiring it like a human brain. It is a series of algorithms which process data by trying to mimic the human brain. It consists of a network of layers of interconnected nodes, in other words call neurons, which process the information that is passed between each other. The connection between each other helps in recognizing the complex pattern within data. Predictions are based on new inputs learned from the past mistakes. It is a process which is useful for recognizing images, human speech and translation between language.

---

[26] AI and Privacy: Risks, Challenges, and Solutions, *Trigyn Technologies* (July 16, 2024), https://www.trigyn.com/insights/ai-and-privacy-risks-challenges-and-solutions.
[27] How Does AI Work? Fundamentals and Step-by-Step Process, *Upwork* (last visited Aug. 14, 2024), https://www.upwork.com/resources/how-does-ai-work.
[28] How Does AI Actually Work? *CSU Global* (last visited Aug. 14, 2024), https://csuglobal.edu/blog/how-does-ai-actually-work.
[29] What is Artificial Intelligence (AI)? Everything You Need to Know, *TechTarget* (last visited Aug. 14, 2024), https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence.

iii. Learning in Dept: It uses that type of artificial neural network known as deep neural networking which contains various number of hidden layers in which data is processed. It allows the computerized machine to go into a state of deep learning, in which it will recognize complex patterns trying to formulate connections and weighting inputs to obtain best result. It is a very important stage as it helps in. Deep learning is particularly effective at tasks like image and speech recognition and natural language processing, making it a crucial component in the development and advancement of AI systems.

iv. Processing of Natural Language: This is a process in which the computer is taught to understand and produce written and spoken language mimicking human beings. It is a combination that consists of computer science, language, machine learning and deep learning, which will help the computer to analyze the text which is unstructured or any voice data and extract relevant information from it.

v. Computer Vision: It is when the machine process through some raw image's videos or visual media from them it will extract an insight it makes use of deep learning and convolutional neural networks to breakdown images into pixels and tag them accordingly, this process helps computers to distinguish between visual shapes and patterns. Artificial intelligence which deals with facial recognition and detection of self-driving cars and robots require such learning.[30]

The above process made it evident that the entire system of artificial intelligence is based on the input of information, in the form of data. The data is collected from life human beings. The concern or fear among the people in society arises, with the question of how safely is their data stored, so that they don't fall prey to unauthorized users and their privacy is violated.

1.4 Surveillance

Earlier times the state had limited resources to be used for surveillance. However with the advancement of artificial intelligence, the state control on the activities of each and every person has increased to such an extent that with just a click they would know all your activities from how much money an individual has in his bank and where he is investing to the extend they would also be aware of the types of political opinion you have. This has created a fear like environment among the people in the society.

Artificial intelligence cyber security technologies have increased and evolved rapidly. It has made various sophisticated tasks like pattern of recognition, anomaly detection very easy and time saving. This has made it very easy for the government to monitor the actions and the moves made by the people. On the other hand, it has a benefit to reduce crime as it will have a more controlled environment from the state, making it easier for detecting crime. However, there is a very picture to it as well. Which, the human beings have become subject to a new type of crime which called as 'cybercrime' and a new type of terrorism has evolved called 'cyber-terrorism.'

The modern era of surveillance of artificial intelligence functions on the technologies of facial-recognition and drones, which have become mainstreamed into public life. However, there are no proper law. In fact, many countries are not even well-prepared laws that would regulate it nor there is any consent from those being surveyed. Digital Surveillance may be cost effective for the state, however on the other hand there is increased vulnerability to the public at large and the cases of biased database and technological leakage have increased to a very large extent. Surveillance not only means surveillance of crime, but it can be surveillance to ever aspect like transaction, health and so on. The breakdown of Covid-19 has not led to concern about health but it has led to a rise in concern about the way extensive surveillance in the name of that state is protecting the healthy from the sick. During that time an individual was barred from public places, if he denied disclosing personal information, whereas disclosure of personal information led to mishandling a lot of data subjecting to private individuals' life. Ultimately causing public-health surveillance conflicting with the public order. It led increases in data burden on the private life of its citizens.[31]

[30] Artificial Intelligence Definition, *Built In* (last visited Aug. 14, 2024), https://builtin.com/artificial-intelligence.
[31]Digital Surveillance and the Threat to Civil Liberties in India, *GIGA* (last visited Aug. 14, 2024), https://www.giga-hamburg.de/en/publications/giga-focus/digital-surveillance-and-the-threat-to-civiliberties-in-india#:~:text=This%20has%20increased%20the%20data,tool%20of%20exclusion%20and%20repression.

During the Kumb Mela that occurred in April 2021, millions of pilgrims gathered at the ghats of Ganga. Artificial intelligence was used which enabled it to zoom on the faces of those who were not adhering to the Corona guidelines and capture it. The method of predictive police of the state along with the invasive surveillance technologies has posed a serious threat on individuals liberties and their right of privacy. All the controls lead to production of large amounts of data, without proper regulation has led to a complete breach of data violation. Ever since the victims of exposure of their personal details has increased leading them to become exposed to cybercrimes.[32] The period between 2019- 2021 the number state used surveillance has increased to a very large extend, the use of technologies like fingerprints, facial recognition is done of ground level of inspection and technologies like CCTV and drones camera with special resolutions are used. For instance, drones were used to detect the crowd who have protested and created violence in the protest of CAA and Farm law in India has been turning as vital public spaces violating the zone of privacy. On the other hand, the police were able to match images with the available database already available like social media and personal identity data, were used to arrest them. However, the charges of faulty data are very high, and it can cause wrongful arrest. After the riots that happened in Delhi, the technologies used for facial recognition only has a 2 percent accuracy rate. [33] Wrongful arrest would result in wrongful detention which is a violation of fundamental right of the constitution of India.[34] Digital Surveillance has created a web of network surveillance, under which every individual irrespective of being innocent is targeted as suspect. Such an attitude is wrong for the smooth functioning of the society and country. Since there must be some sort of level of trust between the state and its citizens. But when the state itself is creating an environment consisting of a sense of fear, such a kind of society can't stand long. With the help of integral surveillance, the individual are monitored pinpointed and profiled without their consent.[35] The act of in-depth surveillance has evolved into an environment in which the collected data have transformed into quantifiable data. Storing and handling data has become business, in the corporate this kind of business is called datafication of individuals. It has created a situation in which a individual is under constant glare under the state and the private companies dealing with it.[36]

It is rightly argued that the state must have some degree of surveillance for fast track of clearing cases. On the other hand, the extent to which such surveillance is for the protection of the society at large and when state is crossing the line and infringing the right to privacy of the individuals? Is a important question. The researcher is of the opinion that, there must be liquidated structure which will decide the balance of interest for national security and safeguarding the right of privacy of an individual. They must go hand in hand, since both are important aspects for the development of society at large.

1.5 Ethical and Legal Framework

The growth of industries like information technology and telecom has caused a revolution since the 1990s. Eventually it led to two consequences, at first it resulted in an increase in digital services and platforms. Secondly, the government recognized that the delivery of online services is a powerful tool that can be used to achieve the objectives of policy, for instance financial inclusion and cash transfer. However growing concerns and sense of insecurity among the society has led to development of digital laws throughout the world.[37] At present we are at a state in which the matter that collection of data can have an adverse effect on the privacy of an individual, is no longer discussed. What is more important and needs to be discussed is that what law needs to be improved to avoid such harm or how law can stop or protect individuals from such harm? In this respect to various legal system have been trying to produce variety of ways to find the answer, it is also trying to harmonize and keep a privacy regulation approach which will match in a globalized system.[38]

---

[32] *Ibid*
[33] Sidharth, *Surveillance Vs. Privacy: Balancing National Security and Individual Rights in India*, 12 Int'l J. Creative Research Thoughts (IJCRT) (May 2024).
[34] Constitution of India art. 22, cl. 1.
[35] Sangeeta Mahapatra, *Digital Surveillance and the Threat to Civil Liberties in India*, GIGA Focus Asia No. 3 (May 2021).
[36] *Ibid*
[37] *Ibid*
[38] Anirudh Burman, *Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?* Carnegie India (2020).

Various countries have tried to create a data protection law which will keep in mind the right of privacy of an individual and keep in mind the present state of technology. The research would like to highlight some countries and their contribution and how they function, which are as follow:

1. **United States of America:** The law that are dealing with privacy are developed and shaped around the conception of privacy as goods, they are designed in such a way that they meet the needs of an innovative environment for the US companies. Therefore, the collection of date by private entities is regulated by the state and federal laws, they will apply on the private entities on sectorial basis. In case there is no law for a specific sector. or the specified law will exclude or is silent upon certain type of component, the one who collects the data is free to collect the data and make use of it subject to the Federal Trade Commission. [39]

Demand for changes in the privacy law has been gradually increasing. Another idea has been slowly rising i.e. the idea of fiduciary duty, which consisted of component like care, loyalty and confidentiality. Which the entity has follow while collecting the data. Since the final purpose of law is to provide a sense of security and freedom in the society at large. Transfer of personal data from one for to the other establishes a legal relationship which arises with the exchange in trust, sensitive data and reliance. The relation that evolves is called the 'Classic Fiduciary Relationship'. The company who collects such data, processes and store the data in vast amounts, creates such a relationship. It is a similar relationship like the relationship between an advocate-client or between a doctor and patient or between banker and his client. In the above mentioned case an environment is evolved between the parties so that they can share their private and sensitive matters that of exposed into to the general public can cause unliquidated loss (unmeasurable loss) to an individual in the sense of reputation and financial status. However, in every part in life we will need people who with the help of their expertise skill can provide us the right and therefore they have a duty of confidentiality.[40] However, there some who may take advantage of this kind of relationship, therefore to avoid such situations we have regulation like court have created the fiduciary duty of care, confidentiality and loyalty which forbids the service giver from abuse of such power. Similarly, such trust responsibilities should be there in ensuring data privacy by the handlers while collecting processing and storing it.[41] If companies like Facebook, Instagram and WhatsApp manipulate the user's ambiguous purpose, fiduciary duties could prevent data collectors from self-dealing, ultimately diverging from the interest of it user[42].

From the above statement the researcher would like to conclude that in the USA the demand for protection in cyber law has diverted to a more relationship-based law. which will also deal in breach of trust. It argued that companies like OLA, Instagram, Wester Union etc. are similarly bound to their clients like Doctor and Patient. They are bound under a strict code of conduct, and they are restricted to act out of their code of conduct. Similarly, it should be applied to the company collecting data and processing data and its clients.

There are end number of cases in the United States in which from time and again right to privacy and the digital era, questioning the integrity. One such landmark case is the Carpenter case. It was a case in which the investigation of armed robbery by the FBI led to identification of several suspects through cell phone tapping and it led them to another participant including Timothy Carpenter. The FBI obtained the records of the carpenter from his wireless carrier, which was under the Stored Communications Act (SCA). The records included the cell-site location information (CSLI), which tracked the movement of the Carpenter's over 127 days. When the matter reached court. The court highlighted various concerns on right to privacy and the digital era which are as follows:

- The court emphasized, on the legitimate expectation of the citizens of privacy in relation to their physical movement as record in the cell-site location information. Such data can reveal in detail information about a person's location overextend period.
- The court rejected the argument made by the government that doctrine of third party, the individuals cannot have a reasonable expectation of privacy for information, which they have given voluntary

[39] Paul Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 Geo. L.J. 115, 132 (2017).
[40] Tamar Frankel, *Fiduciary Law*, 71 Cal. L. Rev. 795, 800 (1983).
[41] *Jack Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, 51 U.C. Davis L. Rev. 1152, 1162 (2018) [hereinafter Balkin, Free Speech].*
[42] Jonathan Zittrain, *Engineering an Election,* 127 HARV. L. REV. F. 335, 340 (2014).

acceptance to third parties like telecom industries including information like cell-site location information. The court held that this argument would make cell-site location information qualitatively different from other types of business record. Since it is more detailed and has a nature of all-encompassing.

- The Court acknowledged that with the help of digital data a more detailed and invasive record of a person's life. Therefor the need of protection through the Fourth Amendment in the technological, for a greater privacy protection.

This case highlights the importance of right to privacy in the digital era. It talked about the step forward for the Fourth Amendment, which will provide protection from various forms of digital data. Suggestion how law enforcement agencies like them can conduct investigations and how the law of privacy can be visualized in an ever-increasing connected world. This case is setting a precedent concerning that law enforcement agencies must obtain a warrant if they are accessing detailed personal digital information. [43]

The above case dealt with a very important question by distinguishing the extent to which a state can conduct surveillance to solve a crime. The researcher would like to highlight that on one hand, it is very important for the law enforcement to have access to data for easily convicting the accused. On the other hand, we have the fundamental right of right to privacy enshrined in our constitution and even in our Human Rights. There is a very thin line between state interference and right to privacy which must be adhered.

There are number of incidents when the law enforcement authority forgets to attain a warrant for the act which is important for the collection of evidence and convict the accused. For instance, in a case the FBI attached a GPS tracking device to the accused care who used to smuggle drugs to catch the peddler. However, this act continued without any warrant. The major legal question that arose in this case was whether installation and use of GPS on the accused car constituted a search under the fourth amendment and therefore required the issue of warrant first? The Supreme Court held that attaching GPS device to a vehicle and using it to monitor the movement has constituted a search investigation and therefore it is important for the law enforcing agency to have a valid warrant from the court. The Court further emphasized the importance of having a balanced law enforcement which is in the interest of individuals privacy right and the rapid technological advancement.[44]

State is not the only one that can make use of data without permission from the actual owner of that data. There is instance in which one data collecting infringed the rights of another data collecting company. In a case where are data analytics company called HiQ Lab used the data available on LinkedIn to create people analytics products, which was used to sell it to other companies/ businesses. Technically it relied on scrapping of data openly available on public profile on LinkedIn. LinkedIn is another profession networking site which is owned by Microsoft. Therefore, when Microsoft became aware of the of HiQ it asked HiQ to stop scrapping the data available on its site. It claimed that HiQ is violating the Computer Fraud and Abuse Act along with various other laws. To protect it user from HiQ, Microsoft has blocked HiQ from access to the data. In this case the question was whether Microsoft is authorized to block HiQ from collecting data which is already openly available in the market of online. The court held that HiQ can continue with the scrapping of data available on public profile on LinkedIn. It also emphasized on that there is a clear distinction between public and private data. In the context of laws relating to computer fraud. The data that HiQ is collecting is already available to the public at large, there is already a presumption of the user his information is visible to the public at large. Hence the user has given permission to see his activity on the platform.[45]

The above has played a significant role in implication for the digital industry, data analytics. It also had set legal boundaries for those industries which do data scraping. It dealt with various issues like keeping a balance of privacy and data ownership. In an era in which large amounts of data is already available on various platforms with. The permission of the actual owner (user).

---

[43] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
[44] *U.S. v. Jones*, 565 U.S. 400 (2012):
[45] *HiQ Labs, Inc. v. LinkedIn Corp*., 938 F.3d 985 (9th Cir. 2019)

The researcher would like to raise certain incidents when we in our daily life receive E-mails, text messages or even calls, as promotion of a certain product or app. What is interesting is that you have never tried to use such product neither have you ever shown your interest for the same. Unlike many Noah's Duguid used to receive text messages from Facebook. However, Duguid never had a Facebook account, nor did he ever submit his phone number on Facebook. Therefore, Duguid filed a lawsuit stating that Facebook is violating the Telephone Consumer Protection Act, as Facebook was sending unsolicited text messages by making use of automatic telephone dialing system without his consent.

It is important to note that the Telephone Consumer Protection Act had made an enactment in 1991 which restricted telemarketing calls and the use of automated telephone equipment. The key issue that arose was in the definition of automatic telephone dialing, in which Telephone Consumer Protection Act described automatic telephone dialing system 'as an equipment with the capacity to store or produce telephone number to be called, using a random or sequential number generator and to dial those numbers." Therefore, the primary issue that arose in this case was 'whether the system of Facebook which is automatically sending text message to phone numbers which is stored in its database, qualifies as an of automated telephone equipment database falling the Telephone Consumer Protection Act.

The Supreme Court held that to qualify the test for an automated telephone equipment database under the Telephone Consumer Protection Act. A device have the capacity to either store a telephone number which can be used has a random or sequential number generator or be able to produce a telephone number using random or sequential number generator.

The decision of Supreme has limited its scope of what can constitute automated telephone equipment database under the Telephone Consumer Protection Act. And according to the above decision the system of Face does not come under the definition of automated telephone equipment database. This judgement made it clear for businesses like Facebook, by providing them guidelines on the use of automated systems for communication on one hand. On the other hand, it made it clear to consumer the type of business that do fall under the definition and therefore come under the Telephone Consumer Protection Act.[46]

The researcher has discussed various incidents which may be a violation of the right to privacy under USA law in general. However, the researcher has observed that there is still a lot of confusion on whether with the help of AI there an infringement of an individual's right to privacy is or not.

There are several regulatory gaps and challenges that United States is facing with the intersection of AI and Right to Privacy. With the rapid development of AI the has been a increasing impact with privacy in ways in which the existing legal framework may not be fully addressed. Some of the key regulatory gaps and challenges are as follow:

- Lack of Comprehensive Federal Privacy Law: In the United States it has been observed that there is a lack of comprehensive federal privacy law. For Instance, in although we have Health Insurance Portability and Accountability Act and Children's Online Privacy Protection Act. However, they do not cover the broader implication of AI on privacy across various sectors. Since there is absence of federal law causing inconsistent protection of privacy across different state and industries. As a result, it many areas of AI are unregulated at the federal level.[47]
- Lack of Regulation of AI in use of Data: To function effectively AI is solely dependent upon the use of large amount of personal data. Currently in the United State the is no legal framework which indebt regulate how AI can make use-process- share this kind of information. As a result it has led to non-consensual data collection ultimately causing miss use of personal data. Causing increase in risk of discrimination and erosion of individual privacy right.[48]

[46] *Facebook, Inc. v. Duguid*, 141 S. Ct. 1163 (2021).
[47] R. Rodrigues, Legal and Human Rights Issues of AI: Gaps, Challenges and Vulnerabilities, *J. Responsible Tech.*, 2020.
[48] *Ibid.*

- Lack of Transparency: The system of AI uses the process of machine learning, which is often opaque making it difficult to understand how they process data and decision making. Since it lacks in transparency it hinders the accountability and therefore undermines the trust.[49]
- Lack of Standardized Ethical Guidelines: Several organizations and guidelines have developed ethical guidelines for AI. However, the is no standardized set of ethical principles that will govern AI and its development across United States.
- Chances of Cross boarder Data Flow and Jurisdictional issue: AI operates across boarders therefore there are chances that a number of jurisdiction will arises. Which will have different privacy regulations creating a challenge in the enforcement. Unlike EU's General Data Protection Regulation. Even companies in US which navigate complex landscape of international privacy laws must have a stricter requirement for trans boarder data management.[50]

The researcher would like to demonstrate that the only possible way to move forward in the US and bridge the gaps is to have a more federal privacy law and specific AI regulations including ethical standards and a stronger enforcement capacity. For smooth and balanced development of society and technology.

2. **Europe:** Throughout European countries, data privacy and data protection are the fundamental rights of their citizens. Therefore, legal protection of such rights are prioritized for every individual over the ease of compliance for companies. The EU follows the General Data Protection Regulation (GDPR), this law deals with normative commitments like the range of individuals rights. It has also created a breadth of its definition and jurisdiction which it will deal with. It has laid down affirmative requirements and laid down grounds for prohibition for the digital industry. [51] It has generated an onus on companies to justify their collection of data and the use of it. By stating the paramount objective of protecting individual right while GDPR completely relies upon the constitutional right of privacy.[52] It places affirmative duties upon the one who are collecting data and create a deterrent environment for those who are trying to exploit their users. Duty of care and loyalty and confidentiality has been crafted in the GDPR.[53]

Once online will remain online. There are several times we upload something on any digital platform; however, it will remain online even though you will not be any more a part of it. A similar incident happened with a citizen from Spain called Mario Costeja González, who filed a complaint with the Spanish Data Protection Agency against a Spanish newspaper called La Vanguardia and Google. His complaint was that there was an old link of the newspaper about real estate auction to the Social Security Debt. It appears always appeared on Googles search engine when his name was searched. The argument laid down by Costeja was that this information is no longer relevant, it is infringing his right to privacy. The question that arose in this case was whether any individual has the right to request search engines to remove links of personal information that is inadequate, irrelevant or no longer relevant under the EU Data Protection Directive 95/46/EC. The Court of Justice of the European Union (CJEU) in this case had established the doctrine of "Right to be Forgotten". The Court held that, since Google is a controller of data and is responsible for processing personal data in search results, it is therefore subject to data protection law of EU. It respect to individuals, it can request the removal of links in relation to their personal data from the search engine. Provided that the data is outdated and irrelevant and it is not overriding the interest of public in data remaining accessible. This case is important as it

[49] N.A. Smuha, From a 'Race to AI' to a 'Race to AI Regulation': Regulatory Competition for Artificial Intelligence, *Law, Innovation & Tech.*, 2021.

[50] *Ibid.*
[51] Schwartz & Peifer, supra note 3, at 122 (calling the GDPR "stunningly influential" on privacy law around the globe).
[52] *Ibid*
[53] Neil Richards & Woodrow Hartzog, Taking Trust Seriously in Privacy Law, 19 *Stan. Tech. L. Rev.* 431, 470 (2016).

not only talk about a balance between AI and but also a balance between right to privacy and the right of public to access information.[54]

The above ruling had played a significant role in the implementation of "global data protection' and its practice. by highlighting the reach of EU data protection law, it has come beyond its borders and is setting a precedent for how companies must handle personal data throughout the world.

Unlike the US, Europe also is facing the challenge to balance the needs of national security on one hand and protection of fundamental rights on the other, particularly when it is dealing with bulk data retention and having the access to personal data. A human right organization called The Ligue des droits humains (LDH), in Belgian challenged the legality of the Belgian Laws that transported EU directives in relation to the data of Passenger Name Record (PNR). Subsequently processing of this data by law and the enforcement authorities, with the purpose of combating acts like terrorism and similar serious crimes. The question in this case in referring to allow the bulk retention and use data of PNR, as it is raising concerns about the compliance with the EU fundamental right. Particularly in respect to private life[55] and right to protection of personal data.[56] Moreover the right to effective remedy.[57]

The Court of Justice of the European Union (CJEU) held that the use of PNR data could be justified in the interest of combating serious crimes like terrorism. However it must be subject to strict safeguards in order to ensure compliance with the fundamental right. The court has further highlighted the following key points:

a. The use of PNR data must be strictly adhered with necessary and proportionate to the legitimate aims pursued. It must be limited to terrorism and serious crime.
b. Indiscriminate and generalized retention of data is not permissible.
c. There must be effective remedies to challenge the retention and use of their data.
d. There must be an effective oversight by independent authority to ensure the use of PNR data along with relevant legal standard and that it is protecting individuals right.[58]

Right to privacy is not only enshrined in the constitution of each country in Europe but it is also enshrined in the European Convention on Human Right. In the landmark case Big Brother Watch and Others v. United Kingdom. [59]The European Court of Human Right Scrutinized the surveillance practice in the UK in special respect of right to privacy, which is enshrined under the European Convention on Human Right.

In the above case, concerns arose with the mass surveillance conducted in UK. This mass surveillance brought light to the Edward Snowden revelation in 2013. It revealed the extensive use of surveillance program being operated by the UK Government Communications Headquarters.it included communication of bulk interception including, intelligence sharing with foreign government. The Applicant along with civil liberties organizations such as Big Brother Watch, the Bureau of Investigative Journalism, and others. laid down the argument that this mass surveillance is violating their rights granted under the European Convention on Human Rights such as follows:

- Article 8 (right to respect for private and family life, home, and correspondence).[60]
- Article 10 (freedom of expression).[61]
- Article 6 (right to a fair trial).[62]

---

[54] *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, Case C-131/12, 2014.
[55] Charter of Fundamental Rights of the European Union, art. 7.
[56] Charter of Fundamental Rights of the European Union, art. 8.
[57] Charter of Fundamental Rights of the European Union, art. 47.
[58] *Ligue des droits humains ASBL v. Conseil des ministres*, C-817/19, [2020] ECLI:EU:C:2020:1034.
[59] *Big Brother Watch and Others* v. *United Kingdom*, 24960/15, [2021] ECHR.
[60] European Convention on Human Rights. art. 8.
[61] European Convention on Human Right. art. 10.
[62] European Convention on Human Right. art. 6.

- Article 14 (prohibition of discrimination).[63]

The court held that, mass surveillance is not inherently unlawful. The bulk interception of communications and intelligence conducted in the regime of UK, sharing violated the European Convention on Human Rights to inadequate safeguards and oversight. Furthermore the court criticized the absence of prior independent authorization for bulk interception warrants and the insufficient oversight of the selection and examination of intercepted materials.

The court further observed that act done by UK's officials is a violation of Artic 8 and 10 of European Convention on Human Rights. The court required UK to implement a mechanism which is more robust and safeguard mechanism to ensure that the surveillance conducted was necessary and proportionate in meeting the standards of human right.[64]

The researcher would highlight that the AI regulation in European Union is much more complex and organized. The above two countries are developed with a well-organized legal structure. The question how countries which are developing deal with their Right to Privacy and AI. The researcher would like to state give the example of India which has come very far in its short span of independence. How it dealt with the development in the world and what issues it has faced. It is important to note that although India has a written constitution with well-defined set of Fundamental rights, however right to privacy not explicitly mentioned anywhere in the fundamental rights.

The intersection of AI and right to privacy in Europe is shaped by a robust regulatory framework, especially in the General Data Protection Regulation. Despite these strong protections, there are still regulatory gaps and challenges. Some of the significant regulatory gap and challenges are as follow:

- Lack of AI Specific Application: Although General Data Protection Regulation provides a strong foundational base for data protection is not designed to tackle unique challenges, which are posed by the AI technologies. [65]
- Chances of Bias and Discrimination: While General Data Protection Regulation does prohibit discriminatory processing of data. There is a limited guidance on how to prevent or mitigate the chances of bias in the system of AI. If no care is taken, there is a possibility that AI driven decision especially in area like hiring, lending and law enforcement can lead to unjust outcome. Therefore, it not only requires regulatory oversight but also the development of best practice for AI fairness.[66]
- Possibility of Trans-Boarder Data Transfer: Although General Data protection regulation has imposed very strict rule in reference to cross board and outside the European Economic Area transfer of personal data. AI is a system which often operates on a global database system, which frequently requires frequent cross boarder data flows. The recent legal border data transfer was impeded with the innovation and collaboration such as the invalidation between EU-US.[67]

The researcher has highlighted the need for the ongoing adaptation of Europe regulatory framework, for effectively addressing the privacy implications of AI. The European Commission even came up with a solution by trying to introduce the Artificial Intelligence Act. The sole purpose of this Act was to address the gaps by introducing the specific regulation for AI all- together focusing on the high-risk application and transparency and accountability

3. <u>India:</u>

In India we don't not have right to privacy explicitly mentioned under the fundamental rights. Therefore, earlier the right to privacy was considered as a right which was used to secure in order to facilitate protection of other fundamental

[63] European Convention on Human Right. art. 14.
[64] *Big Brother Watch and Others v. the United Kingdom* (Applications nos. 58170/13, 62322/14, and 24960/15, 2021)
[65] B. Goodman & S. Flaxman, European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation," *AI Mag.*, 2017, available at ojs.aaai.org.
[66] N.A. Smuha, E. Ahmed-Rengers & A. Harkens, How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act.
[67] A. Chiappetta, Navigating the AI Frontier: European Parliamentary Insights on Bias and Regulation, Preceding the AI Act, *Internet Policy Rev.*, 2023, available at econstor.eu.

rights. With the recognition of right to privacy under Article 21 of the constitution of India, it has transformed to an end itself.[68]

The effect of modern technologies throughout the world has also cause conscience in in countries like India. In India the concern of data protection was influenced with the introduction of the General Data Protection Regulation (GDPR). Therefore, in 2018 NITI Aayog in collaboration Digital India and the Ministry of Electronics and Information Technology, has classified 5 expert members. In which it outlined its national strategy in five major sectors, which are, Healthcare, Agriculture, Education, Smart Cities and Infrastructure, Smart Mobility and Transportation in which AI will provide credential support to them, with the purpose of fulfilling economic and social development.[69] the researcher would like to bring the readers notice that the above plan of AI Strategy is more focus on development, growth, job and creation of skill development rather than on privacy issue and how personal data of citizens is to be protected

The draft of "the Personal Data Protection Bill, 2018" was submitted which was an initiative conducted by the government and Ministry of Electronics and Information Technology. This committee was headed by Justice Srikrishna. The aspiration of this bill was to regulate violation of privacy, and it can take within its jurisdiction and business, enterprise, which deals with the part of collection of personal data of its users. It furthermore classifies data into a separate category called "sensitive personal data. Such data can be processed only with the explicit consent.[70]

In countries like India, it is important to keep in consideration the low literacy rate leading to lack of awareness about data privacy. Therefore, is the law enforcement may become complex and difficult as well. Since the complex nature of AI makes even highly qualified people fall prey to data privacy. Since India the diverse demographic it possesses a very big challenge for the government of India to conduct awareness programs with limited resources.[71]

The law that directly regulate AI and may affect the development or use of AI in India. Even a Few scattered laws like Information Technology Act 2000 along with Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011, have been replaced by the Digital India Act 2023. Although it is still in draft form.[72]

However it is important to note no such specific law is presently there in the society, therefore the researcher is just try to demonstrate the vision of the government to develop a law through the Digital India Act 2023, which will cope with the difficulties and vulnerabilities that the society will face with AI and their privacy

There are several factors why the Bill on Digital India Act 2023, has still not be passed are as follows:

1. The Complexity of the issues involved, the nature dealt under the IT Act and the nature that the Bill is try to address is quite vast. Therefore, crafting legislation that effectively addresses these complex issues while balancing innovation, privacy, and security is challenging and requires careful deliberation.

- The Bill must be aligned with other recent and upcoming legislations, such as the Data Protection Bill and amendments to existing laws like the Indian Penal Code and the Evidence Act. It is important for proper coherence between the Bill and the different laws for proper regulation.

[68] *Justice K.S. Puttaswamy v. Union of India*, WP (C) 494/2012 (2012)
[69] National Strategy for AI: Discussion Paper, NITI Aayog, available at https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf.
[70] The Personal Data Protection Bill, 2019.
[71] Akshita Jain, AI: A Threat to Privacy?, 1 *Indian J.L. & Legal Rsch.* 1 (2021).
[72] AI Watch: Global Regulatory Tracker – India, White & Case, available at https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-india.

- Since AI is transboundary the government of India must take due consideration the international development and meet the global standards.[73]

Although there have been several cases which have from time and again questioned the state to bring stringent laws in terms of digital privacy. Such cases show that the general citizen of the country is becoming aware about the risk factor evolving privacy. A similar incident occurred when the project of Aadhar, which was introduced by the government. In this project, it was mandatory for the applicant to submit a biometric identification. When the matter went to court. it was argued that such collection of sensitive data, is a violation of right to privacy which is a fundamental right under the constitution of India. The court held that the right to privacy is not only a fundamental right but also intrinsic to the right to life which is guaranteed under Article 21 of the constitution. Another important consideration which was made, is that right to privacy is not only subject to a single dimension but it is subject to multiple dimensions which included the bodily autonomy, informational privacy and the right to make personal decision without the fear of interference. However, it is not absolute. Therefore, the state has the autonomy to restrict it, subjecting that any such restriction must satisfy the test of legality and proportionality. Although the court has explicitly dealt with the right to privacy, however it failed to decide the constitutional validity of Aadhar project itself.[74]

The failure of the above case gave rise to another which question the integrity of the right to privacy in criminal investigation and the authority of the state to gain access to data from Aadhar. It not only questioned the protection provide under the constitution of India but also the privacy protection which was guaranteed under the Aadhar Act of 2016 and the right to privacy recognized by the Supreme Court Justice K.S. Puttaswamy (Retd.) v. Union of India judgment. The Supreme Court in this case held that the Aadhar data cannot be shared with the State (CBI) or any investigating agency without first gaining permission under the Aadhar Act 2016. The court reiterated the importance of providing protection of privacy with sensitive data like biometric data and therefore such kind of data cannot be overridden in the absence of legal mandate. The Aadhar Act 206 clearly states that under certain circumstances the data can be shared but the state must get prior approval of the District Judge. The court has noted that this procedure was not followed by the CBI. The court in its judgement showed a very clear understanding that there will be a case of national security. However, even in such a situation the state or investigating agency must comply with the procedural safeguards laid down by the law. so that the right to privacy is not infringed.[75]

The Researcher would like to divert the readers mind to another angel, the incident of agreement of data sharing between WhatsApp and Facebook. In 2016 the Supreme Court dealt with another important question which was the 'legality of sharing data between WhatsApp with its parent company Facebook. In 2014 when Facebook acquired WhatsApp data sharing such as phone numbers and analytics, with Facebook and other group companies for various purposes, including targeted advertising began between the two companies. Although the Supreme Court decided to hear the case with other similar case and decide upon the matter of right to privacy as a fundamental right.[76]

The regulations in India that are dealing with AI and right to privacy is still at a very nascent stage. The are several factors and challenges that are needed to be addressed which are as follows:

[73] Transparency Must Be a Cornerstone of the Digital India Act, *Tech Policy Press*, available at https://www.techpolicy.press/transparency-must-be-a-cornerstone-of-the-digital-india-act/.

[74] *Justice K.S. Puttaswamy (Retd.) and Anr. vs. Union of India and Ors.,* (2017) 10 SCC 1.
[75] *Unique Identification Authority of India v. Central Bureau of Investigation,* (2020) 7 SCC 1
[76] *Karmanya Singh Sareen v. Union of India*, (2016) 10 SCC 15.

- Lack of a comprehensive Data Protection Law: There is no comprehensive data protection law at present in India all are proposed bill it is still expected to become a law. leaving a huge regulatory gap. Without clear legal framework, there is an increase in chances of misuse of personal data and gross violation of privacy.[77]
- Data Localization and Cross- Border Data Transfer: India proposed very stringent data localization mandating certain type of data must e stored within the country. However, the implication of these requirements for AI is often relying on the data flow, which are not fully addressed.[78]
- Chances of Bias and Discrimination: the system of regulating AI in India is vulnerable to biasness and discrimination, specially with trained biased data base. There is a lack of regulatory guidance on how to identify prevent and mitigate biasness.[79]
- Lack of Awareness and Expertise in AI Ethics: In India there is limited awareness of AI ethics, in both aspects from the side of the policy maker and the general public in India. Ultimately leading lack of understanding of the ethical implication of AI technologies and the need for protection of privacy.[80]

Conclusion

Artificial Intelligence has integrated into every facet of modern life. It has drastically altered the landscape of privacy. On one hand AI has brought unprecedented advancement across various sectors, from healthcare to enforcement of law. On the other hand, it has also introduced various challenges in respect to preservation of privacy of an individual. Development of AI technologies specially dealing with data collection, surveillance and decision making, has raised various critical and serious concerns on how this information is collected, processed, stored and used.

The researchers in this paper have discussed various existing legal frameworks including the General Data Protection Regulation and other proposed legislations in countries like India. Despite of it they often fail in adequately addressing the challenges posed by AI in protection of privacy. As there are gaps in the regulations and transparency and the transgression of ethical guidelines, all these issues have aggravated the situation more. Leaving individuals becoming easy prey to data breaches, surveillance, and algorithmic bias.

There is an urgent need for enacting a robust regulatory legal framework, which will regulate the development of ethical AI practices. Since protection of privacy can be strengthened only through legal frame works which will prioritize transparency fairness and accountability while dealing with AI. There are several stakeholders like the government and tech companies, who must collaborate and work together to ensure the right to privacy. AI is a part of modern society and therefore the only feasible answer would be that there must be a balance between the protection of privacy and the rapid innovation of technologies, so that one can benefit AI while mitigating the potential risk.

[77] Governing Artificial Intelligence: Ethical, Legal and Technical Opportunities and Challenges, *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, available at https://doi.org/10.1098/rsta.2018.0080.
[78] *Ibid.*
[79] Asif Khan, The Intersection of Artificial Intelligence and International Trade Laws: Challenges and Opportunities, 32 *IIUMLJ* 103 (2024).
[80]