Page 425 - 432 **DOI:** *https://doij.org/10.10000/IJLMH.115364*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 4

2023

Balancing Privacy and AI: Legal and Ethical Consideration

ANANYA SHRI SINGH[1]

ABSTRACT

In the 21st century where the paramount importance to the technology or the area of machine learning, the emergence and development of the artificial intelligence and related system has been in discussion these days. Think of a time when you enter a hospital and you see no doctor instead you see robotics to carry out the treatment. Isn't that interesting but what if the same has life threatening effects on your body. Before diving deeper into Artificial intelligence and its implication on data privacy it becomes significantly important that we understand what artificial intelligence, what is the greatest power we humans are entrusted with it is the capacity and ability of the human brain to think and understand. So artificial intelligence does the work of carrying out the task that humans can do, they try to replicate the abilities of the human mind but artificially.

With Ais as an emerging power, it is important to regulate the Artificial intelligence since we are surrounded with AI and we are depending on AI for the completion of our task in one way or the other. The scariest part of the system is that the computer system uses our stored data in order to ease our work. The Ais algorithm learn from our earlier data's and most of the time such data is used by the countries to spy on their citizens. This is where the problems or room for negative consequences arise. There is hardly any legislation that deals with such a risky issue. The apex court has itself reiterated that right to privacy is a fundamental right under Article 21 of the Constitution of India. Therefore, it becomes the need of the hour that we understand the problems that are occurring in the global sphere through the use of artificial intelligence and hence it is high time that we need proper framework to ensure that regulations are suggested to prevent future deterioration of the conditions in this emerging field of Artificial intelligence.

Keywords: *Technology: Artificial Intelligence: Computer Algorithms: Human Mind.*

I. INTRODUCTION

In the world where the technological advancement has led to the emergence of new field that is artificial intelligence which is surrounding us every now and then. We are living in the world where the artificial intelligence has assumed more power and is interfering in every sphere

[1] Author is a student at Indore Institute of Law, Indore, India.

 [ISSN 2581-5369]

where earlier humans used to work or carry out task which was almost unimaginable a decade ago. These technologies have become a vital part of life and hence touching every sphere of our lives. There is no denying the fact that this artificial intelligence system will change the way we live, will transform our lives to an extent that is almost impossible to think or imagine, the transformation may be such that our humankind existence will be at stake, possibly there are chances that the artificial intelligence may overshadow humans' capacity and ability to think.

The most striking part of using such Artificial intelligence system is when you use such system much of the time you are unknowingly or unwillingly reveal your personal information or data such as your location, your other data that is stored in your computer or other devices. The tracking companies what they actually do they use your data and customize your data to affect your online working and experience.[2]It is interesting that we have an access to almost every information that is there on the internet. It must be easy and might not look offensive before your search your desired information: but what happens if you are attacked by the ad suggesting what you were searching for, what makes such thing pop onto your screen, let dive deep into the reality and see how it works.

(A) Artificial intelligence

"Artificial Intelligence" is a term that has been first coined by Mr. John Mc Carthy. The recent developments or advancements in this field can be seen when more emphasis is laid on faster computers, faster machine learning and faster data processing. All these functions that eventually lead to efficiency and less time consumption has convinced the tech giants or world leaders in the fields of technology to make large investments. The task that a human brain is known or supposed to perform is when performed by the computer programs or robots there the room for the term artificial intelligence open, so artificial intelligence is basically replicates the doing of the work what can be done by a human brain but in less time.

(B) Artificial intelligence and its two distinct natures

Artificial Intelligence is supposed to make our work or business transaction more effective and easier, in its long run it might prove to be a threat since the information that is being feed into the AI-driven algorithm is more susceptible to breaches. There are chances of AI being able to process or form data on the basis of earlier data that is being stored without the consent of the person whose data is so processed. For instance, facial recognition technique, biometric data are more invading our privacy to a great extent.

[2] ThinkML, www.thinkml.ai (15th June, 2023)

 [ISSN 2581-5369]

II. ARTIFICIAL INTELLIGENCE AND PRIVACY RELATED ISSUES

(A) Privacy and its invasion

The privacy is one such term that has been used in ancient times as well, the code of Hammurabi, in the passages of bible, in the Hebrew culture also the right to privacy was acknowledged and hence was given importance. The word privacy is not confined just one sphere but it has various facets for instance, bodily privacy, data privacy, personal information privacy territorial privacy and so on.

Freedom has been entrusted upon the citizen to use his information in whatever manner he likes to use it, no other person can intrude upon ones right to privacy. Various scholars have tried to define the term privacy. Westin is of the view that privacy is the claim of an individual to determine what information about himself, he wants to share with the others. Fried defines Privacy in terms of the control that one can have over the information about oneself.[3] Richard Posner, an American jurist and economist refers 15 to privacy in terms of withholding and concealment of information.[4]

(B) Global sphere framework for right to privacy

The protection and observance of human rights is of utmost importance and numerous global organisation have tried to preserve these rights the most important of all of them is the right to privacy, the Universal Declaration for Human Rights has imbibed in its article 12[5], Covenant on Protection of Rights of Child, 1966 (Article 17)[6], Article 14 of the International Convention on the Protection of all Migrant workers 1990[7], European Union Data Protection directive[8] all these international conventions and declarations tends to protect the privacy rights of the people in global sphere. European Union directive has set a benchmark for countries in the entire globe as they formulate regulations to preserve and protect the personal information, countries that are not part of the EU have decided to get inspired to frame laws so that the right of privacy cannot be intruded.

(C) Recognition of privacy rights in India

a. What about personal data protection and where is it defined

[3] History and Definition of Privacy, Passeidirecto (15th June, 2023), www.passeidireto.com.
[4] Ibid.
[5]Yacine Ait Kaci (YAK)), Universal Declaration of Human Rights, page no. 26, 2015, www.udhr.org.in.
[6] United Nations Treaty Collection, www.treaties.un.org. (16th June, 2023)
[7] International Convention on the protection of the rights of all migrant workers and members of their families, www.ohchr,org (16th June, 2023).
[8] Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *L 281, P. 41 – 50, 1995*, www.eur-lex.europa.eu

i. The personal data protection bill, 2019

As earlier studies provide us with an overall idea that personal data of an individual must be ensured, the Indian legal framework acknowledges the protection of personal data in the Personal Data Protection Bill, 2019 which was the outcome of the recommendation of the Justice Sri Krishna Committee which was constituted after the landmark judgement in K.S Puttaswamy v. UOI case.[9]

As also mentioned in European GDPR, the is duty of the data fiduciaries that they process and preserve the personal information which may include health data, biometric data, financial data or other categories of data in a proper, specific and in lawful manner.[10] Now here the Indian citizens are entrusted with right which includes right of withdrawal of their consent, they even the right to raise question on their processed data. Here in the bill much emphasis has been laid on the consent of its citizens, it is after their explicit consent only the data is supposed or can be processed either in the country or outside. There is certain critical information that is supposed to be processed in India only.

There are penal provisions for such non-compliance to protect the data therefore the privacy breach has given paramount importance these include a fine of Rs. 15 crore or 4% of the annual turnover of the fiduciary whichever is higher, processing of data without consent attracts imprisonment for a term of up to three years or fine or both.[11]

ii. Privacy Protection under The Information Technology Act, 2000

Section 66E of the Information Technology act, 2000 acknowledges the right to personal data protection or simply privacy in accordance with the act, a person who knowingly or intentionally publish, transmit or process image of a person without his consent is said to a breach on the privacy of the person, and can be imprisoned for a term which may extend up to 3 year or a fine of Rs. 2 lakh or both.[12]

Under Section 43A of the Act,[13] it become and make mandatory for the corporate bodies to process, publish or transmit the data that is highly ‘sensitive personal data’. Here the data must be handled with due diligence in case of such failure with the said provisions the corporate bodies would be held liable and certainly they have to compensate the party whose data had been mishandled by them.

[9] Justice KS Puttaswamy (Retd) v. UOI, AIR 2017 SC 4161.
[10] Article 4-11, The Personal Data Protection Bill, Bill of the Parliament, 2018 (India).
[11] Karnika Seth, Personal Data Privacy: Overview of Justice Srikrishna Committee Report, Pg. 360.
[12] The Information Technology Act, 2000, Section 66E, Acts of the Parliament, 2000 (India).
[13] The Information Technology Act, 2000, Section 43A, Acts of the Parliament, 2000(India).

 [ISSN 2581-5369]

iii. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

The consent of the data subject needs to be taken in writing before the collection of sensitive personal data.[14] The data so collected must be such that it is collected not forcibly but freely. The application of consent before the collection of personal data is significantly narrowed by the fact that the Rule 5 applies only to sensitive personal data or information and not all kinds of personally identifiable information.[15]

(D) Decided Cases on Privacy & Data

Here in the instant case the regulation 236 of the Uttar Pradesh Police Regulation which stated that police may visit at the domicile place of person was held to be violative of Article 21[16] and the apex court held that the provision is unconstitutional as to the fact that Article 21[17] safeguards the right to privacy of its citizen.[18] However further it was held that the restriction can be imposed but only on the condition that it must be in accordance with the procedure established by law.[19]Here it needs to be noted that information that is published in view of the fact that becomes significant to draw the picture of past events is not a case of breach of privacy.[20]

In Auto shanker case[21], it was held by the court that right to privacy is guaranteed under Article 21 of the Constitution, no one can publish anything with respect to the person concerned and if he does such malicious act, he is liable to pay for the damages that have incurred upon the person so concerned due to breach of his privacy.[22]

Again, right to privacy was questioned and the constitutional validity of the Aadhar was challenged in the case of Justice KS. Puttaswamy v. UOI,[23] the nine – judge bench held that every citizen of India has the fundamental right to privacy which may be covered under Article 14, 19 and 21. The apex court has from time to time widened the scope of privacy one such instance is where the petitioner prayed before the court to remove the name of his daughter from

[14] Rule 5 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011(India).
[15] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011(India).
[16] J.N Pandey, Constitutional Law of India, 57th edition (2020).
[17] India Const. art. 14.
[18] Kharak Singh v. State of Uttar Pradesh AIR 1963 SC 1295.
[19] Gobind v. State of Madhya Pradesh (1975) SCC (Cri) 468.
[20] Khushwant Singh v. Maneka Gandhi, AIR 2002 Del 58.
[21] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632.
[22] J.N Pandey, Constitutional Law of India, 57th edition, pg. no. 293 (2020)
[23] Justice KS. Puttaswamy v. UOI, AIR 2017 SC 4161: (2017) 10 SCC 1.

 [ISSN 2581-5369]

the search engines of various high court and court website as it may affect married life, the court considered the point and stated that in consonance with right to be forgotten in sensitive cases that involve to affect the modesty or reputation of the person so concerned.[24]

III. ETHICAL CONSIDERATION OF ARTIFICIAL INTELLIGENCE ON BEACH OF PRIVACY

(A) Principles of ethics that must be ensured while designing artificial intelligence

a. Respect, protection and promotion of human rights and fundamental freedoms and human dignity

It is pertinent to note that an individual is supposed to live happily when he lives in an environment where his rights whether basic or fundamental are entrusted upon, where there is recognition of such rights and where there is almost no room for any exploitation. The Artificial intelligence system must be designed in such a way that a man lives his life with dignity, his personal information is not disclosed without his explicit consideration or consent so that his image in the society is not at stake.

b. Environment and ecosystem flourishing

The actors involved in the process of designing artificial intelligence system must ensure that they comply with international as well as national laws on climatic issues, the ais must be used in a way that should not deteriorate the condition of the environment, this can be done by reducing the pace at which such developments are made since the radiations so emitted cause deteriorating effect on the environment, flora and fauna.

c. Ensuring diversity and inclusiveness

Respect, protection and promotion of diversity and inclusiveness should be ensured throughout the life cycle of AI systems, consistent with international law, including human rights law. This may be done by promoting active participation of all individuals or groups regardless of race, colour, descent gender, age, language, religion, political opinion, national origin, ethnic origin, social origin, economic or social condition of birth, or disability and any other grounds.[25]

d. Living in peaceful, just and interconnected societies

The humankind existence is based on the fact that they love in peace-loving environment and society which looks the same at all people, the societies must not be segregated as the

[24] Karnika Seth, "The right to be forgotten on internet", 2021.
[25] Artificial intelligence - recommendation on ethics, www.unesco.org/en. (17th June, 2023)

 [ISSN 2581-5369]

interconnected societies form the foundation stone of a nation state and hence it becomes imperative that the emerging field of artificial intelligence system should not segregate, objectify, or undermine the autonomy of any particular community which will result in turning of one community against the other, or might threaten the coexistence between humans.

(B) Ethical Challenges posed by Artificial Intelligence

a. Bias and Discrimination

While designing Artificial Intelligence system the designer must feed data that is non-discriminatory and lack of biasness, the system training must be such that there is literally no room for any kind of biasness, for example an AI used for hiring might discriminate against certain groups if the data it was trained on contained such discrimination. Addressing bias in AI requires careful consideration throughout the AI development process.[26]

b. Transparency

Usually, AI with deep machine learning is called 'Black boxes' since the internal working of the Artificial Intelligence becomes almost impossible to understand which has negative implication, therefore it becomes vital that the actors of the system must lay emphasis on clear understanding of the working and ensure that the work so designed is transparent to understand.

c. Evil Genies. (Unintended Consequences)

In order to fulfil the needs, the artificial intelligence tends to come up with terrible and unintended consequences, for example – Imagine the system has been asked to eradicate cancer in human body, the unintended consequence that the system will provide us with will be to eradicate the very fittest of survival, seems very scary right?

d. Misused Accelerated Hacking

The system tends to understand our data that is earlier and utilises the same by the designer to hack various platforms across the world of internet, here again it is pertinent to note that data that we think is safe is actually not, it is sometimes used by such system to spy on us, the data so stored is processed and used without the consent of the person whose data is so utilised.

e. Singularity

The designers work in this field to lessen their task but there are instances where such robots or deep machine learning turn against their mastermind, so there is this potential risk if we will not check this overshadowing power of the system.

[26] Yancy Dennis, Artificial Intelligence-privacy and ethics, Medium (17th June, 2023) www.medium.com

 [ISSN 2581-5369]

IV. WAY FORWARD

The emergence of such technology has made or lives way better and simple as it was a decade ago, the digitalization of every field has posed certain challenges that makes it the need of the hour to regulate such system otherwise the negative implications are very much clear to see, the self-mechanised car that have proved to be life-threatening, the use of artificial intelligence devices such as Alexa, where there was such instance of spying on by the use of facial recognition technique.

The systems should be allowed only to collect relevant data, because the more sensitive data is spread across worldwide web there are more chances of misuse and hacking of personal information. It has been found that 73% of the users tend to share their sensitive personal data with the system that have more transparency and credibility in the market. The consumers of such service must be informed in what manner their information can be used.

Visibility system must be created under which the usage of such processed or stored data must be made available to the person whose data is so consumed. In essence, the creators should be more responsible in how they handle customer data, and customers should be more careful about the information they share with brands. Meanwhile, one would expect to see more data protection regulations springing up around the world. Europe has taken a major step with the GDPR, and that needs to be replicated in other countries and regions.

V. CONCLUSION

There has been no saving of time if we had no artificial intelligence technology, our way of lives has become far better in today's time, the projects can be made in almost no time, we can reach a place through the use of google maps, since childhood the child is subjected to technology, in today's era most of the time we are surrounded by the technology and ultimately this has led to the advancement of the field of Artificial Intelligence.

However, on the contrary there are various instances mentioned above such use of technological advancement can pose a serious threat to our privacy, as directly and indirectly we have the right to live with dignity therefore the personal information is supposed to be protected as far as possible, more legal and ethical framework must be established in order to delete any kind of room for such negative and terrible consequences.

*****

 [ISSN 2581-5369]