INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 3 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A STUDY ON IMPACT OF ARTIFICIAL INTELLIGENCE ON RIGHT TO PRIVACY IN INDIA

AUTHOR - ROHITH S B & SETHUPRIYA N, STUDENT AT THE TAMIL NADU DR.AMBEDKAR LAW UNIVERSITY

BEST CITATION - ROHITH S B & SETHUPRIYA N**,** A STUDY ON IMPACT OF ARTIFICIAL INTELLIGENCE ON RIGHT TO PRIVACY IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 4 (3) OF 2024, PG. 170-177, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT:

Artificial Intelligence (AI) is a concept which is an intelligence artificially exhibited by computer systems which were previously unique to mankind. It is the ability to imitate humans, such as using language, image, recognition, making predictions, learning, problem-solving, ability to move and manipulate objects on their own by computers. Huge volumes of data are crucial for AI system. The AI algorithms can analyze and provide solutions to complex problems without any human interference. Through machine learning, AI systems are fed with data from pre-existing datasets that by using algorithms that helps in predicting the desired output. The data includes locally available data from end users of any platform which are all connected through the Internet. The data may be public or private data. The AI sorts out the sensitive personal data from inferencing other data which infringed the privacy rights of an individual. With growing modernization and integration of AI into different sectors, it has benefitted in lots of way. However, the easy access to the personal data by AI has raised legal and ethical difficulties which requires for ensuring a balance between technology and fundamental rights. The fundamental right of privacy envisaged under Article-21 of the Constitution of India has been a major concern in the digital age of AI. Since there is no proper legal framework which specifically governs AI related legal issues, there is need for a comprehensive legal framework to regulate and provide for safeguarding the privacy rights of an individual. The evolution of privacy and laws relating to it and the impact of AI on privacy in India will be discussed in this article.

KEYWORDS: Artificial Intelligence, Constitution, Data, Digital, Privacy

INTRODUCTION:

The rapid development and advancement of AI technologies has brought about significant benefits, but also posed great challenges to the fundamental right to privacy. The constitution of India protects the right to privacy under Article 21. The AI system relies on collection and processing of large amount of personal data, which can potentially infringe upon privacy rights of an individual. The techniques used in AI like machine learning and deep learning algorithm can uncover patterns and insights from data that may reveal sensitive personal information.

Further AI driven surveillance, facial recognition and predictive policing technologies raise concerns about mass monitoring and profiling. Though personal Digital Personal Data Protection Act, 2023 has been passed which aims to regulate the processing of personal data and proposes safeguards like data localization and individual consent requirements, it lacks in addressing issues specific to AI system. As India embraces digitalization and AI across sectors, the policymakers must address the privacy implications. Robust governance framework, ethical guidelines, regulatory mechanisms are needed to ensure AI development aligns with constitutional rights. Striking the balance will be vital for promoting responsible AI that enhances societal benefits without compromising individual privacy.

With AI as an emerging power, it is important to regulate the Artificial intelligence since we are surrounded with AI and we are depending on AI

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 3 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

for the completion of our task in one way or the other. 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.

This project discusses about the concept of AI and privacy, their evolution in digital era and impact of AI on right to privacy of an individual.

ARTIFICIAL INTELLIGENCE:

The term "Artificial Intelligence" was first coined by Mr. John McCarthy. He defines AI as "the science and engineering of making intelligent machines". Recent developments in this field can be seen where emphasis is given on faster computers, faster machine learning, and faster data processing. Artificial Intelligence is science of making machine to do things that would require intelligence if done by men[358].

Artificial Intelligence is the ability to imitate humans and teaching machines to learn, think, decide, make predictions, solve problem, and act as humans would. It refers to some kind of ability for machine to learn, reason, sense, plan, build some kind of perception of knowledge and communicate it in language or speech, vision or image recognition[359].

AI is combination of technologies which includes

i. Deep learning
ii. Big data analysis
iii. Robotics
iv. Block-chain
v. Internet of things, which requires high computing facilities, storage, network infrastructure, security, etc.

AI system can complete complicated tasks without explicit programming because they are built to learn from data, adapt to new inputs and improve over times.

NATURE AND SCOPE OF ARTIFICIAL INTELLIGENCE:

There are two distinct features of AI. AI is supposed to make work for humans more effective and easier. The utility of Artificial Intelligence is increasing rapidly. There are numerous innovations done in the field of AI. Some of the instances where it has consistency in its usage all over the world are:

i. Google maps, weather forecast
ii. Applications like Ola, Uber, Rapido, etc., for traveling purpose
iii. Robots
iv. Facebook, Instagram, Snapchat
v. Online shopping apps
vi. Smart assistants like Siri, Alexa
vii. Online payment portals.

The development of AI is being done because it is helpful and making things work in much easier and simpler way. There is a chance for AI to process or form data based on earlier data stored without the permission of the person whose data is processed. Examples are facial recognition, biometrics. There are various challenges which the people and society needs to face with regards to it which includes data privacy, patent and copyright issues on AI modules, National security, contractual protections, etc.

RIGHT TO PRIVACY:

Privacy is an age-old concept. It is derived from a Latin term 'Privatus', which means separate from rest. Privacy is the wish to remain unnoticed. Though humans are social animals, there some aspects of life that a person wishes to keep it hidden or share with a selected number of people. V S Justice Brandeis says that privacy is an individual's "Right to be left alone". Nariman J says that "the dignity of the individual encompasses the right of the individual to develop his or her full potential". This advancement can only take place if an individual has autonomy over fundamental decisions and control on dissemination of

[358] Sheshadri Chatterjee and Sreenivasulu, Evolution of AI and its impact on human rights, International Journal of Law and Management, Vol 64 Issue 2, 2022 Pg 184-205

[359] Anuttama Banerji, AI and right to privacy concerns and implications, @ https://governbetter.co

personal data that can be violated by unauthorized use of this data[360].

Privacy as a human right is enjoyed by every human being by virtue of their existence. Privacy can also extend to other aspects, including bodily integrity, personal autonomy, informational self-determination, protection from state surveillance, dignity, confidentiality, compelled speech, and freedom to dissent or move or think[361].

Privacy is recognized internationally in various conventions:

i. Article 12 of Universal Declaration of Human Rights, 1948
ii. Article 17 of International Covenant on Civil and Political Rights, 1966
iii. Article 16 of Convention on the Rights of the Child, 1989
iv. Article 8 of the European Convention on Human Rights

These legal instruments protect against 'arbitrary interference' with an individual's privacy, family, home, honour, correspondence and reputation.

RIGHT OF PRIVACY IN INDIA:

In India, the right to privacy was not directly envisaged by the framers of the Constitution and was not a part of Fundamental Rights. The judiciary has interpreted privacy through various judgments since 1954. In M P Sharma vs Sathish Chandra case[362], the Supreme Court of India decided in favour of the practice of search and seizure when contrasted with privacy.

In 1962, the case of Kharak Singh vs. State of U P[363]was examined by the Court relating to power of police surveillance with respect to 'history sheet' which was the personal record of the criminals under surveillance. The petitioner argued that night domiciliary visit to his house by the police was violating his fundamental right to move freely across India. The court ruled that domiciliary visits do infringe the petitioner's rights. But also, the court ruled that right to privacy was not a fundamental right. So, the police surveillance did not infringe his rights.

In 1975, the Supreme Court of India introduced the Compelling State Interest test from the American jurisprudence in the case of Gobind vs State of M P& Anr[364]. The court stated that right to privacy of an individual would have to give way to larger state interest, the nature of which must be convincing. With time, the domain of privacy has expanded and it has come to incorporate personal sensitive data such as medical records and biometrics.

In 1997, the Supreme Court in the case of PUCL vs Union of India[365], famously known as Telephone tapping case, unequivocally held that individuals had a privacy interest in the content of their telephone communications.

In 1998, Mr. X vs Hospital[366], the Supreme Court held that privacy isn't absolute as it has some exceptions. Thus, it can be observed that the right to privacy was recognized through a series of cases, but their exceptions were also given due place.

In the 21st century, questions with respect to the right of privacy have centered on Aadhaar, a government scheme in which residents get a unique ID after giving their biometrics like fingerprints, iris scan and demographic details.It is a system that does not require permission, allowing the user to choose whether to participate or not for both unique identification and related services[367]. Aadhaar was challenged in court for violating privacy. The Supreme Court in 2013 ordered it to be used only in public distribution system and LPG subsidy only. In October 2015, the Supreme Court extended the use of Aadhaar to deliver certain services, but no person should be deprived of any services.

[360] Apoorva Thakur, Right to privacy vis-à-vis AI: Indian scenario, IJLMH, Vol 7, Issue 2, Pg 3370, (2024) at. https://www.ijlmh.com.
[361] Krishnadas Rajagopal, The lowdown on the right to privacy, THE HINDU, (August 26, 2024) https://www.thehindu.com/news/national/the-lowdown-on-the-right-to-privacy/article19386366.ece.
[362] AIR 1954 SC 300
[363] AIR 1963 SC 1295
[364] 1975 SCC (2) 148
[365] 1997 SC 568
[366] 1998 (8) SCC 296
[367] AI and privacy and its impact on personal data, THE ECONOMIC TIMES, https://m.economictimes.com

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 3 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

In 2017, Justice K Puttaswamy (Retd) vs. Union of India[368] was landmark judgment given by the Supreme Court stating right to privacy is a fundamental right. This case challenged the validity of Aadhaar biometric scheme on the ground that it violates the right to privacy. A 9-judge bench ruled that right to privacy is a fundamental right for every citizen of India under Article 21 of the Constitution of India. The court adopted specifically adopted three criteria that must be met before any Article 21 right can be infringed upon

i. Legality based on existing laws
ii. Necessity based on legitimate state objective
iii. Proportionality that guarantees a logical connection between the object and means used to attain them[369].

It is a landmark judgment because it emphasizes privacy as an individual right. The right to privacy can be clubbed in a three-part right

i) Right to bodily and mental integrity
ii) Right to decisional autonomy
iii) Right to control over personal information.

The judgment notes that the consent of individual is paramount to any state programme based on data collection and data mining. Privacy is not an absolute right as it involves certain justified restrictions like fulfillment of welfare functions of the state, controlling crime and meeting its other legitimate goals by the State.

The Information Technology Act, 2000 was amended in 2008 to insert Section 43 A which made companies compromising personal data liable to pay compensation and framed 8 rules to protect privacy of an individual.

NEXUS BETWEEN AI and RIGHT TO PRIVACY IN DIGITAL AGE:

The use of AI technologies is inextricably linked to the right to privacy. As technology continues to advance at an unprecedented rate, the use of artificial intelligence has become increasingly prevalent in many areas of our lives. AI has the potential to revolutionize the way we interact with technology[370].

AI is understood as the capacity of a computer-controlled robot or application to act in ways often associated with human intelligence and computers are programmed to mimic human intelligence in areas such as thinking, finding meaning, making generalizations, and learning.

Privacy is the right to keep personal information confidential and free from unauthorized access. Privacy is crucial as it protects individuals from harm of identity theft, helps to maintain autonomy, personal dignity, respect, control over personal information, free will and free from fear of surveillance.

In digital era, personal data has become a valuable commodity. The amount of data we generate and share online grows exponentially which enable various entities to gain new insights and make better decisions with the use of that data.

With the ever-increasing presence of digital technologies in daily life and the influence of the physical and virtual worlds, an individual's private sphere extends beyond their physical private space. AI system does not only rely on vast amount of the private data of public for their development, but they are being deployed in ways that rupture the private sphere. Due to this, the issue of privacy is pressing in the digital age.

AI has become essential instrument to help humans manage their hectic lives and get tasks done faster and more efficiently. AI has to rely on vast amount of data to train their algorithm and improve performance, problem solving and predictions. The main privacy concerns surrounding AI is the potential for data breaches and unauthorized access to personal information. There is a risk that all the data

[368] AIR 2017 SC 4161
[369] Aditi Prabhu, Artificial Intelligence in the context of the Indian Judicial System, Bar and Bench, www.barandbench.com
[370] Nick Lawrence, AI in UI, 2323 and Beyond, Medium(28th August, 2024) https://uxplanet.org/ai-in-ui-2023-and-beyond-346b4602eff7

collected, processed, stored would fall into the wrong hands, either through hacking or any other security breaches. Therefore, the right to privacy is being violated implicitly.[371]

IMPACT OF AI ON RIGHT TO PRIVACY:

In this modern technological world, AI is omnipresent. As AI evolves, it can make decisions based on subtle pattern in data that are difficult for humans to notice. AI present a challenge to the privacy of individuals because of the complexity of the algorithm used in AI system. It requires a vast amount of personal data, if it falls into wrong hands, it can be used for malicious purposes. The methods used by AI to collect and process data presents serious privacy concern because individuals are not aware of how the data is being used. There are various ways in which AI impacts the right of privacy:

- **Data Exploitation**:
  Users are often uncertain about the amount of data that they create process or divulge, and how they are collected and utilized. They are also unaware of how the AI exploits the data[372]. With the help of varied algorithms, AI can predict sensitive information from non-sensitive forms of data. For example, keyboard typing patterns of a person can be used to deduce their emotional states like nervousness, confidence, sadness, and anxiety[373].
- **Identification and Tracking:**
  AI can be used to identify and track individuals by mapping their daily routine activities by accessing personal data from different devices like smart phone and smart watches. AI differentiates the personal and non-personal data by de-anonymizing the anonymous data of the individuals based on inferences from other devices. Modern systems can create 360-degree profiles of citizens by stitching together data from street cameras, card transactions, and social media profiles.[374]
- **Inference and Prediction of information:**
  Predicting private information from publicly available data is a common use of AI and ML system. Machine Learning is often deployed to comprehend and predict people's emotional status by analyzing their sensitive personal data from unrelated data. Such profiling poses a significant challenge to privacy.
- **Profiling:**
  It is simple to exploit and misuse information gathered by AI profiling. The person whose personal information is being gathered does not know anything about it. Profiling to sort, score, categorize, assess and rank individuals and group is done by AI. The consent in such cases is implicit when individuals are accessing the applications or software. This also poses a threat to privacy of an individual.
- **Voice and Facial Recognition:**
  The use of voice and facial recognition technology (FRT) directly infringes on the right to privacy and free assembly. FRT has been increasingly used by States to track and watch their citizens, indirectly for the purpose of national identity system, or crime reduction, or more explicitly to track dissidents. Sometimes it is used to identify, harass and arrest peaceful protestors. Ex: It was primarily granted by the High Court of Delhi in Sadhan Haldar vs NCT of Delhi,[375] for the purpose of finding and reuniting missing

[371] Dr. Mark Van Rigmenam, Privacy in the age of AI risk, challenges and solution, @ www.digitalspeaker.com (22 August 2024)
[372] Artificial Intelligence in Legal Profession in India, Bar and Bench, www.barandbench.com, visited (14th August 2024)
[373] Michael Deane, AI and the Future of Privacy, Towards Data Science (August 27,2024), https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4
[374] Yuvraj Malik, Privacy risk: Report says India among 75 nations with AI surveillance tools, Business Standard (August 27, 2024), https://www.businessstandard.com/article/current-affairs/privacy-risk-report-says-india-among-75-nations-with-ai-surveillance-tools-119112700134_1.html
[375] Anushka Jain, The Delhi Police must stop its facial recognition system, Panoptic Tracker, (August 27, 2024) https://panoptic.in/case-study/the-delhi-police-must-stop-its-facial-recognition-system

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 3 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

children. But however, Delhi police used FRT to arrest protestor of Citizen Amendment Act, 2019. Use of FRT has been implemented without individual's consent which violates the right to privacy.

- **Mass Surveillance:**

  AI powered surveillance system is capable of continually monitoring huge populations which enable pervasive and intrusive monitoring of people's daily activities. AI surveillance tools are being used more often by government around the world for a range of objectives, including law enforcement, national security, and public safety. While this technology is used for crime prevention and investigation, they also present serious issue with the privacy rights of individuals.

- **Bias and Discrimination:**

  While designing AI 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. An AI used for hiring might discriminate against certain groups if the data was trained on contained such discrimination. Addressing bias in AI requires careful consideration throughout the AI development process[376].

SOLUTIONS TO OVERCOME AI CHALLENGES ON RIGHT TO PRIVACY:

As technology is constantly growing, we are continuing to integrate AI into various aspects of our lives. It is clear that privacy is becoming increasingly important. Organization and companies that use AI must prioritize privacy in their AI system's design and implementation.

- TRANSPARENCY in data collection and usage, how the algorithm works, and handle user data to personalize experiences should be made.
- INFORMED CONSENT is essential before collecting and using a user's personal information for prediction, personalization, etc. Consent should be freely given, specific, informed and unambiguous.
- DATA MINIMIZATION is essential to prevent the accumulating of unnecessary or irrelevant data. AI system should only gather and store the required data only based on the service required. It reduces the risk of data breach.
- DATA SECURITY measures are essential to protect personal information from breaches and illegal access by AI system. Strong encryption of personal data can help mitigate the risk of data breach.
- PSEUDONYMIZE THE DATA: Pseudonymizing is replacing personal identifiable information with artificial intelligence. It helps in securing privacy.
- ACCOUNTABLE and ACCESSIBLE: Users must have access and able to review, amend, and remove their personal information and preferences.
- FAIRNESS and Non- DISCRIMINATION: AI algorithms should be created without prejudice or discrimination that everyone should be treated equally.
- PRIVACY AWARENESS: Users must be educated and employees should be trained about how to secure the privacy of individuals collected data.

CONCLUSION:

Though it poses substantial obstacles to the protection of privacy rights, the emergence of artificial intelligence has great potential for social amendments. Due to fast digitalization and growing integration of AI in India among various sectors, the government must take aggressive measures to address potential

[376] Yancy Dennis, Artificial Intelligence- privacy and ethics, Medium(28th August, 2024) www.medium.com

privacy concern. It will be vital to find the optimal equilibrium between fostering innovation and safeguarding fundamental rights such as right to privacy.

To guarantee that AI developments respect the right of privacy of individuals, effective checks and balances, privacy protection in AI development, increasing transparency and accountability are crucial elements. There must be a balance between advancing technology and upholding fundamental human rights which will pave a way for a time when AI is used ethically and responsibly for the benefit of all.

Decentralized AI technologies offer a promising way forward by enabling secure, transparent and accessible AI services and algorithms. By leveraging these platforms, we can reduce the risks associated with centralized systems while promoting greater regularization and accessibility of AI solution. It is important that governments and regulatory bodies take an active role in overseeing the development and deployment of AI technologies. This includes the establishment of regulations, standards, and oversight bodies that can ensure the responsible and ethical use of AI while also protecting the individual's privacy rights. '

Ultimately, protecting privacy in the digital age if AI requires collaboration and cooperation across a range of stakeholders, including government, industry, and civil society. By working together to develop and implement strategies that promote privacy and security, it ensures that AI benefits are realized in a manner that is ethical, responsible, and sustainable and respects the privacy and dignity of all individuals.

REFERENCE:

1. Sheshadri Chatterjee and Sreenivasulu, Evolution of AI and its impact on human rights, International Journal of Law and Management, Vol 64 Issue 2, 2022 Pg 184-205
2. Anuttama Banerji, AI and right to privacy concerns and implications, @ https://governbetter.co
3. Apoorva Thakur, Right to privacy vis-à-vis AI: Indian scenario, IJLMH, Vol 7, Issue 2, Pg 3370, (2024) at. https://www.ijlmh.com.
4. Krishnadas Rajagopal, The lowdown on the right to privacy, THE HINDU, (August 26, 2024) https://www.thehindu.com/news/national/the-lowdown-on-the-right-to-privacy/article19386366.ece.
5. AI and privacy and its impact on personal data, THE ECONOMIC TIMES, https://m.economictimes.com
6. Aditi Prabhu, Artificial Intelligence in the context of the Indian Judicial System, Bar and Bench, www.barandbench.com
7. Nick Lawrence, AI in UI, 2323 and Beyond, Medium(28th August, 2024) https://uxplanet.org/ai-in-ui-2023-and-beyond-346b4602eff7
8. Dr. Mark Van Rigmenam, Privacy in the age of AI risk, challenges and solution, @ www.digitalspeaker.com (August 2024)
9. Artificial Intelligence in Legal Profession in India, Bar and Bench, www.barandbench.com, visited 14th August 2024
10. Michael Deane, AI and the Future of Privacy, Towards Data Science (August 27,2024), https://towardsdatascience.com/ai-and-the-future-of-privacy-3d5f6552a7c4
11. Yuvraj Malik, Privacy risk: Report says India among 75 nations with AI surveillance tools, Business Standard (27 August, 2024) https://www.businessstandard.com/article/current-affairs/privacy-risk-report-says-india-among-75-nations-with-ai-surveillance-tools-119112700134_10.html

12. Anushka Jain, The Delhi Police must stop its facial recognition system, Panoptic Tracker, (August 27, 2024) https://panoptic.in/case-study/the-delhi-police-must-stop-its-facial-recognition-system

13. Yancy Dennis, Artificial Intelligence-privacy and ethics, Medium(28th August, 2024) www.medium.com