IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 3, April 2024

Study on Artificial Intelligence – Exacerbated Privacy Threat: Legal Consideration

Vaishnavi Shekhar Pawar
LLM (Criminal Law) 1st Year 2nd Sem.
School of Law, Sandip University, Nashik, Maharashtra, India

Abstract*: AI is not imminently replacing jobs due to its advanced capabilities, but recent generative AI applications like ChatGPT have made significant strides in AI history. India lacks a comprehensive regulatory regime for privacy rights and data protection, but the Information Technology Act, 2000 and the Personal Data Protection Bill, 2019 aim to protect individual rights and establish a regulatory body. India has launched a national program on AI (NPAI) to harness the potential benefits of AI and transformative technologies. However, the digitization of personal information has led to a conflict between privacy and data protection. Data protection laws are needed to regulate and process data, protect individual rights, enforce privacy and security rules against unauthorized access, and impose penalties for non-compliance. AI systems are reliant on personal data, which poses risks to data privacy, including potential privacy violations, biases, discrimination, and data misuse. To minimize the risks to data privacy, individuals, organizations, and governments must take steps to protect personal data from privacy violations, biases, and misuse.*

Keywords: Artificial intelligence, Right to Privacy, The Digital Age, It Act, Digital Protection Act**.**

I. INTRODUCTION

AI technology, including virtual assistants like Siri and Alexa, autonomous vehicles, and facial recognition systems, has raised concerns about personal data privacy. AI systems often rely on vast amounts of personal data to train their algorithms and improve performance, including sensitive information such as medical records and social security numbers. The collection and processing of this data raises concerns about how it is being used and who has access to it. The main privacy concerns surrounding AI are the potential for data breaches and unauthorized access to personal information. With so much data being collected and processed, there is a risk that it could fall into the wrong hands, either through hacking or other security breaches. Generative AI can be misused to create fake profiles or manipulate images, and cybercrimes affect the security of 80% of businesses across the world.

AI has the potential to revolutionize our lives, but it also raises privacy concerns. As AI becomes more prevalent, it can collect and analyze vast amounts of personal data, which can be used for both positive and negative purposes. It can also be used for surveillance and monitoring, such as facial recognition technology used by law enforcement. To ensure compliance with GDPR, AI algorithms should be designed to minimize data collection and processing while maintaining security.

As AI technologies advance, they can collect and analyze significant amounts of data about individuals, including behaviors, preferences, and thoughts and emotions. This information can be used to make predictions, target individuals with advertising or marketing messages, or make decisions about access to services or opportunities. However, AI systems may perpetuate existing biases and discrimination, particularly in areas like employment. To address these concerns, AI technologies must be developed and deployed responsibly, ensuring data collection and processing is transparent, secure, and with clear guidelines for usage and sharing.

II. MEANING ARTIFICIAL INTELLIGENCE (AI)

AI uses technology to automate tasks that normally require mature, human-like intelligence. In other words, when people perform the same tasks, they need to use various higher-order cognitive processes. While this definition is based on '*human*' intelligence, the Organization for Economic Co-operation and Development ("**OECD**") had defined AI in

DOI: 10.48175/568

2019 pursuant to the latter's underlying *technical* traits – *i.e*., as a machine-based system that is designed to operate with varying levels of autonomy, and which can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.[1]

Historical Background of Artificial Intelligence

Thousands of years ago, when ancient philosophers were debating matters of life and death, the concept of "artificial intelligence" first emerged. In ancient times, inventors made things called "automatons" which were mechanical and moved independently of human intervention. The word "automaton" comes from ancient Greek, and means "acting of one's own will."One of the earliest accounts of an automaton dates back to 400 BCE and mentions a mechanical pigeon built by a Plato buddy. One of the most well-known automatons was built by Leonardo da Vinci around the year 1495, many years later.

History Of Right To Privacy

The Indian Supreme Court with nine-judge bench under JS Khehar, ruled on 24 August 2017, that the right to privacy is a fundamental right for Indian citizens per Article 21 of the Constitution and additionally under Part III rights. The court specifically adopted the three criteria that must be met before any Article 21 right can be infringed upon: legality (i.e., through an existing law); necessity (i.e., a legitimate state objective); and proportionality (i.e., a rational connection between the invasion's intended goal and the methods used to achieve it) **Gobind v. State of MP (1975):** This is the decision where the Supreme Court was again faced with a similar question of right to privacy. The facts of the case were such that it dealt with police surveillance by domiciliary visits. The Supreme Court recognised the significance of the right to privacy but said that it should give way to a larger state interest. It states that the right to privacy has its own set of restrictions, such as public order, morality, national security, etc.

Internet Freedom Foundation v. Union of India (2019): Considered to be another landmark decision in the realm of the right to privacy, the case dealt with the issue of internet shutdowns and how they impact the right to privacy. The Supreme Court held that the suspension of internet services is against our fundamental rights and must not be permitted unless they adhere to the principles of necessity and proportionality.

III. CURRENT FRAMEWORK IN INDIA

The threat of AI replacing jobs is not imminent due to the current task-oriented systems being too sophisticated and lacking human reasoning and logic. This is consistent with previous AI commentators who claimed that existing AI demonstrates a narrow intelligence.

However, recent generative AI applications, such as ChatGPT, have made significant strides in AI history by following instructions, processing human prompts, and writing text. These applications are built using foundation models, which contain expansive artificial neural networks, like neurons in the human brain. These models represent a revolutionary change within deep learning, capable of processing large and varied sets of unstructured data and performing multiple tasks.

As on date, India does not have a specific and comprehensive regulatory regime dealing with privacy rights and data protection. However, the constitution of India provides privacy rights guaranteed under the scope of Article 21 but it is not enough to provide adequate protection to the data in this digital age because of the essentially sectoral nature of the existing frameworks. The relevant provisions of Information Technology Act, 2000 regulates the use of sensitive personal information. Recently, in 2019 legislature ha introduced a new bill called 'The Personal Data Protection Bill, 2019' with an aim of protecting the autonomy over the personal data of the concerned individual and to further set up a specific regulatory body that will deal with personal data infringement activities[2] India has launched a national program

[1] RajatSethi , Deborshi Barat and RohinGoyal , *India*: *Regulating Artificial Intelligence In India: Challenges And Considerations* https://www.mondaq.com/india/privacy-protection/1339066/regulating-artificial-intelligence-in-india-challenges-and-considerations

[2] Abhishek Das, *Right to privacy and data protection in digital age: Possibility of myth?* https://www.lawyersclubindia.com/articles/right-to-privacy-and-data-protection-in-digital-age-possibility-of-myth--10682.asp

on AI ("NPAI") to harness the potential benefits of AI and similar transformative technologies. The national AI portal, 'INDIAAI, acts as a content repository for this purpose. In May 2023, a report on generative AI was published, focusing on economic impacts and other important consequences.

IV. TECHNOLOGY STANDS IN VIOLATION OF PRIVACY.

The digitization of personal information has led to a conflict between privacy and data protection, two major internet governance issues. Data protection is a legal safeguard that ensures privacy, while data privacy suggests how personal information should be handled based on its perceived importance. It is crucial to be aware of privacy rights when sharing personal information to avoid multiple.

Data is easily available from credit card numbers, Aadhar or PAN cards, bank accounts, and social security numbers. The history of privacy highlights that when data gets into questionable hands, bad things might follow. Therefore, there is a need for Data Protection Laws to regulate and process data, protect individual rights, enforce privacy and security rules against unauthorized access, and impose penalties for non-compliance with prescribed policies. The United General Assembly passed a resolution in 2018 on the right to privacy in the digital age, calling for global concern on human rights. Privacy is a fundamental human right recognized in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other human rights conventions. The appointment of the 1st UN Special Rapporteur in 2015 on the Right to Privacy in the Digital Age reflects the need to address privacy rights issues at global and national levels. In the age of digitalization, the right to privacy has become a challenging issue as personal data is routinely collected and traded in the new economy.The growing prominence and usage of AI systems have led to a complex and multifaceted issue regarding data privacy. AI systems, designed to analyze and process large amounts of data, are inherently reliant on access to personal data, which poses several risks to data privacy.

One of the primary ways AI systems impact data privacy is through their reliance on personal data, which includes names, addresses, and other identifying information. This data is then processed by the AI system, which uses it to make decisions, predict outcomes, and identify patterns. The sheer scale of data processing and the sensitive nature of the data involved create a significant risk

V. DISCUSSION

Data privacy for AI systems is a critical issue, requiring robust security measures to prevent breaches and unauthorized access. Transparency is crucial for accountability and user trust, as AI models can be complex and difficult to explain their decisions. Obtaining clear consent for data collection and use can be complex, as users may not fully understand how their data will be processed. Additionally, AI systems can inherit biases from training data, leading to discriminatory outcomes. Addressing bias and ensuring fairness in AI algorithms remains a continuous challenge.

AI is revolutionizing the way people access and find information online, with platforms like social media and search engines increasingly using AI systems to control user engagement. While some uses may seem harmless, others can have serious repercussions, such as self-censorship and altered behavior in public spaces and private communications. Techniques like video surveillance, facial recognition, and behavior analysis are being used by public authorities and private companies to hinder freedom of expression and infringe on the right to privacy. Mass surveillance is disproportionately interfered with, while targeted surveillance may only be justified when prescribed by law, necessary for a legitimate aim, and proportionate to the desired outcome.

AI content moderation systems can potentially censor legitimate speech if not trained on slang or nonstandard expressions used by minority groups. The impact of AI on freedom of expression is sector- and context-specific, with different issues depending on its application. Digital technology shapes how people exercise their right to freedom of expression, access information, and interact online. Technical standard setting bodies like the Institute for Electrical and Electronics Engineers (IEEE) are developing standards for ethical and safe AI systems.

Civic space is the physical and legal place where individuals realize their rights, and AI applications are shaping decision-making systems and spaces where people and communities organize, associate, and assemble. Media pluralism and media freedom are essential for protecting and promoting freedom of expression in a globalized, digitized, and converging media landscape.

DOI: 10.48175/568

Protection of freedom of expression and information requires a strong legal framework, effective mechanisms for protection, due process of law, and active networks of institutions and activists.

VI. CONCLUSION

The integration of AI into Indian law is gaining momentum, with collaboration between legal professionals and AI systems crucial for effective use. AI is designed to complement lawyers, not replace them, and presents challenges to intellectual property laws, necessitating the evolution of existing legal frameworks. Legal ethics in the context of AI are crucial, with law schools offering practical training on using AI tools for legal research, contract analysis, document review, and due diligence. AI holds the promise of enhancing efficiency and accessibility of legal services, but the legal community must guide this transformation while upholding fairness, transparency, and accountability. Lastly, AI systems pose a risk to data privacy through the potential for data misuse. For example, an AI system designed to analyze financial data could use personal data to make decisions about loan applications, credit ratings, or insurance policies. If this personal data is not properly secured or used unethically, it could result in privacy violations, including the unauthorised release of sensitive information.AI generates content, inventions, or works. One of the most prominent issues is the ownership of AI-generated content. In the case of Juventus FC v. Blockeras, the Rome Court of First Instance granted an injunction to Juventus FC, restraining Blockeras from selling NFTs and Action Cards featuring images of Christian Vieri wearing a trademark.

Copyright is a critical issue in AI-generated content, as the creator typically holds the copyright. However, there is no clear legal framework on this issue, and the originality of AI-generated debate.

Patents are also a concern, as AI-generated inventions must meet novelty, non-obviousness, and utility criteria to be patentable. Determining who owns the rights to an AI-generated invention can be complex, especially when the AI system is operated by an organization.

In conclusion, the impact of AI on data privacy is a complex and multifaceted issue that requires careful consideration and a proactive approach from individuals, organizations, and governments. By taking steps to protect personal data from privacy violations, biases, and misuse, we can ensure that the benefits of AI are enjoyed by all while minimizing the risks to data privacy that come with this powerful technology

REFERENCES

[1]. Kumar S Dr, Kaur G Dr , Cyber Laws and Cybercrimes (2021- Fifth edition) .
[2]. Duggal P Dr , Cyber Law (2023- Third edition)
[3]. Sharma V (, Information Technology Law and Practice (2023 –fifth edition).
[4]. Karnika Seth , Computers, Internet And New Technology Laws (2021- third edition)
[5]. Https://Www.Mondaq.Com/India/Privacy-Protection/1339066/Regulating-Artificial-Intelligence-In-India-Challenges-And-Considerations
[6]. Https://Www.Lawyersclubindia.Com/Articles/Right-To-Privacy-And-Data-Protection-In-Digital-Age-Possibility-Of-Myth--10682.Asp
[7]. Https://Ainowinstitute.Org/Ai_Now_2017_Report.Pdf,
[8]. Https://Www.Technologyreview.Com/S/604087/The-Dark-Secret-At-The-Heart-Of-Ai/.
[9]. Https://Ash.Harvard.Edu/Files/Ash/Files/Artificial_Intelligence_For_Citizen_Services.Pdf