Online ISSN 3007-3197
Print ISSN 3007-3189
http://amresearchreview.com/index.php/Journal/about

Annual Methodological Archive Research Review
http://amresearchreview.com/index.php/Journal/about
Volume 3, Issue 4(2025)

The Impact of Artificial Intelligence (AI) on Privacy Rights: An Analytical Exploration

Rehan Ullah[1]

Article Details

ABSTRACT

Artificial intelligence (AI) is transforming daily life and industry in modern society. This paper examines how advanced AI technologies affect privacy rights. We begin by examining AI's transformative effects across sectors in modern society. Next, the right to privacy protections is explained. The paper then discusses AI applications and privacy rights. We examine how AI surveillance and facial recognition technologies, while improving security and efficiency, pose privacy risks through unwarranted monitoring and data collection. Voice recognition and speech processing technologies are also examined, showing how they improve user experience but raise data storage and misuse concerns. This article offers a nuanced view of how AI affects privacy and proposes ways to protect individual rights in a digital world.

Rehan Ullah
International Islamic University, Islamabad Pakistan. Email: Rehanullah782@gmail.com

INTRODUCTION

Artificial Intelligence (AI) is a turning point in the twenty-first century, impacting every sector from health to education to the judicial system. All those things that were considered impossible or difficult became effortless as a result of the artificial intelligence revolution. Certain areas of AI require personal data to function properly, such as demographic data, contact information, behavioral data, health data, financial data, communications data, sensor data, social data, preferences data, and professional data.

The rise of technology and artificial intelligence raised grave concerns about privacy, which is considered a fundamental right. There are potential benefits to artificial intelligence, but we must not overlook the considerable risks that come with it. This article delves into the concept of feeding personal data to AI, as well as the benefits and potential concerns of artificial intelligence in data collection, processing, and storage. It examines the legal, ethical, and technological aspects of artificial intelligence, as well as its complex link to privacy concerns.

The Role of Artificial Intelligence in Modern Society

"Artificial Intelligence is the science of making human intelligence in machines."[1] Artificial Intelligence is the field of computer science that aims to mimic human thinking and learning processes. AI is the study of creating intelligent machines that can perform all of the tasks that require human intelligence, such as speech and voice recognition, natural language understanding and decision making. In simple terms, AI systems are artificial intelligence devices that is capable to do some things the human brain can do which means that the devices possess the cognitive abilities.[2]

AI is a collection of different techniques that develops intelligent behavior in machines, a few basic and main techniques are described below.

Machine Learning: Machine learning is a subfield of computer science that develops algorithms that learn and improve its performance with experience.[3] It is a subtype of artificial intelligence (AI) that learns from integrated data and improves in performance with time. In simpler terms, it is a method to make a computer think like a human being. For example, machine learning algorithms are used to replicate a human's natural ability, such as captioning

[1] McCarthy, J. (2007). *What is artificial intelligence?* Stanford University. http://www-formal.stanford.edu/jmc/
[2] Swan EJ, Artificial Intelligence Law (2024).
[3] Fong RC, Scheirer WJ and Cox DD, 'Using Human Brain Activity to Guide Machine Learning' (2018) 8(1) Scientific Reports.

photos, driving a car, playing a game, and so on.

Natural Language Processing (NLP): Natural language processing (NLP) is a subfield of computer science and artificial intelligence (AI) that uses machine learning to helps computers in communicating and understanding with human language.[4] Language translation, auto-prediction Popular websites like Google rely on NLP to translate and grammatically correct a sentence. Virtual assistants such as Siri and Alexa use Natural Language Processing (NLP) to receive, comprehend, and provide responses to user orders. Natural Language Processing (NLP) functions as an email filter, similar to Gmail, using it to sift through spam messages and classify emails into main, social, and promotional categories appropriately.

Robotics: Robotics enables artificial intelligence for locomotion. They are machines furnish with artificial intelligence having the ability to perform tasks autonomously and semi autonomously that generally require human intelligence AI technologies can be utilized in a wide range of robotic applications, including supporter and caring robots (including humanoid ones), autonomous land, air, and sea vehicles, swarming robots, search and rescue robots, service and manufacturing robots, robotic toys, various military robots, and intelligent prostheses. The different elements of AI, including speech recognition, precise manipulation, autonomous navigation, machine vision, pattern recognition, and localization and mapping, serve essential functions. These functions are enhanced by fundamental capabilities of advanced artificial intelligence, such as acquiring knowledge from past experiences and predicting the result of a particular action.[5]

Artificial intelligence provides the essential opportunities by leveraging and utilize it to drive positive outcomes in several sectors such as education, healthcare and finance etc., but the potential hazards shouldn't be ignored because it may also pose a serious threat.

UNDERSTANDING THE RIGHT TO PRIVACY

The definition and legal meaning of privacy is "the right that determines the nonintervention of secret surveillance and the protection of an individual's information."[6] The right to privacy in simple terms means that a person shall not be subjected to unwanted publicity. Privacy encompasses multiple dimensions, including information privacy, bodily privacy, privacy of

[4] IBM, 'What is NLP (Natural Language Processing)?' (no date) https://www.ibm.com/topics/natural-language-processing accessed
[5] Bogue R, 'The Role of Artificial Intelligence in Robotics' (2014) 41(2) *Industrial Robot* 119.
[6] The Law Dictionary, 'Privacy' (no date) https://thelawdictionary.org/privacy/

communications, and territorial privacy.[7]

The right to privacy is a fundamental human right enshrined in several international conventions and treaties. Article 12 of the Universal Declaration of Human Rights (UDHR) states that *"no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to attacks upon their honor and reputation. Everyone has the right to the protection of the law against such interference or attacks"*. While it is further stated in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) 1966 that, *"(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks"*. If we go through the above provisions of UDHR and ICCPR, it may be concluded that the legal provisions are in accordance for the era of telegrams and papers; that was a time when this digital and technology revolution was unimaginable, but the time has evolved and the technology has emerged in the society. The boundaries and limitations of right to privacy are difficult to define under these provisions. Due to this technological revolution, the provisions defined by the previous human rights treaties and conventions are no longer considered applicable. The concept of privacy has now been broadened to encompass not just individuals but even states. Surveillance, data collection, data analysis, profiling, facial recognition technology, voice and biometric data, and other activities all contribute to the broadening of privacy rights. The need for a more comprehensive interpretation of privacy is felt in the digital era because technology evolves daily.

Solove categorized privacy into six distinct classifications in order to provide a comprehensive comprehension of the right to privacy that is relevant across various historical periods.

(1) The right to be left alone and not to be bothered.

(2) Limited access to the self, Protecting the safety of one's personal information, preventing unauthorized access or disclosure

(3) Secrecy, the deliberate practice of hiding certain information or concerns from others

(4) Control over personal information, the capacity to exercise authority over personal information

(5) Personhood, the preservation of ones' personality, individuality and dignity and;

[7] Jain SA and Jain SA, 'Artificial Intelligence: A Threat to Privacy?' (2019) 8(2) *Nirma University Law Journal.*

(6) Intimacy, exercising authority or imposing limits on one's personal relationships or parts of life.[8]

AI APPLICATIONS AND THEIR IMPACT ON PRIVACY RIGHTS

Data is collected in the artificial intelligence to enhance the efficiency, precision, and efficacy of the AI system. Artificial intelligence systems are more proficient in learning from data and performing more successfully when there is a larger amount and higher quality of user information available.[9] But the incorporation of AI in several areas of modern life has the potential to impact the fundamental right to privacy, thereby impacting the right to dignity. In the Pakistani Constitution, the right to dignity is the only fundamental right that is not subject to any legal restrictions.

The emergence of artificial intelligence has significantly altered industrial labor, created novel opportunities for innovation, and enhanced old ones. Nevertheless, complications linked to artificial intelligence are escalating on a daily basis, posing a concerning problematic for the modern day. The issues associated with the integration of artificial intelligence include biases, lack of impartiality, unemployment, and privacy concerns.

AI SURVEILLANCE AND FACIAL RECOGNITION

The word "surveillance" has been derived from French which means "watching over". In simple terms the surveillance is the act of monitoring and observing individual or groups of people for the purpose of care and control. Therefore, AI Surveillance is the use of artificial intelligence technology to observe and analyze human actions for many objectives, including security, law enforcement, and marketing even monitor people's emotional states in public spaces. The internet and artificial intelligence have significantly decreased the cost of big data in analytical applications. Cameras are now found in every corner of our daily existence. As we stroll through the streets, our every step is constantly monitored by AI surveillance, leaving people with no means of bypassing the persistent collection of personal information.[10] The approach entails using sophisticated algorithms and machine learning methodologies to analyze vast quantities of data and detect patterns or irregularities in human behavior.[11] The surveillance

[8] Solove DJ, *Understanding Privacy* (Harvard University Press 2010).
[9] Bartneck C and others, 'Privacy Issues of AI' in *SpringerBriefs in Ethics* (Springer 2020) 61–70.
[10] *Security, Ethics, and Privacy Issues in Artificial Intelligence' (CSDN, 7 July 2022)* https://blog.csdn.net/weixin_45859485/article/details/125658756
[11] Spair R, 'The Ethics of AI Surveillance: Balancing Security and Privacy' (LinkedIn, no

footage is analyzed in real-time using visual data collection and analysis methods, detecting anomalies, recognizing faces, and identifying objects of interest.[12]

In public health surveillance, AI and reliable data management platforms effectively analyze massive infectious diseases, predict trends, and support public health responses that manage contagious diseases and prepare for future health crises. In security and safety surveillance, the AI-assisted system enhances the protection of public places, improves the security and safety of public spaces by monitoring suspicious movements and thereby aiding in the prevention of crime. Additionally, the AI system in industrial surveillance enhances the operational efficacy of services across industries by monitoring for faults and optimizing them through AI video surveillance. While the, AI facial recognition technology is increasingly proving to be an easier alternative in the modern world. This technology utilizes the process of analyzing and matching facial traits obtained from real-time cameras, videos, and images to accurately recognize and distinguish individuals. The AI facial recognition system can be applied to address security concerns, regulate access to electronic devices, and enhance marketing efforts. For example, airport counter cameras facilitate the process of examining and identifying passengers, while retailers commonly employ them to personalize the shopping experience.

Although the AI surveillance system and facial recognition system has several advantages, it is crucial to be mindful of the potential privacy and data risks it poses. These technologies are based on visual data collection and analysis, as well as machine learning algorithms, to extensively collect and evaluate personal information through cameras installed in various locations. There are concerns regarding the ongoing and immediate monitoring of individuals using facial recognition technology, which constantly tracks and monitors them at all times. Authorities and private entities have the ability to store and analyze extensive records of individuals over time, enabling them to monitor people's actions and interactions. This practice of AI surveillance undermines individuals' anonymity in public spaces and places where they expect complete privacy, while also infringing upon their right to privacy.

In the ACLU v. Clearview AI case, Clearview AI, a company, collected around 3 billion

date) https://www.linkedin.com/pulse/ethics-ai-surveillance-balancing-security-privacy-aiethics-spair--sc2pe/ accessed 26 July 2024.

[12] Towards Analytic, 'All About Vision Analytics: Extracting Insights from Visual Data with AI' (31 July 2023) https://www.towardsanalytic.com/all-about-vision-analytics-extracting-insights-from-visual-data-with-ai/

faceprints from publicly accessible images, which were then utilized for secret tracking and surveillance. However, the company has been alleged by the ACLU and ACLU of Illinois, among others, of violating privacy rights under the Illinois Biometric Information Privacy Act (BIPA). This act mandates that individuals whose data is being shared with others must be notified and be asked for their consent. Unfortunately, the company failed to comply with these requirements and provided access to the database to private companies, wealthy individuals, and various law enforcement agencies without informing the individuals affected. The court got to a conclusion, resulting in a settlement agreement that prohibited Clearview services throughout the United States. Additionally, the court barred them from providing faceprint databases to any entity in Illinois, including state and local police, for a period of five years.[13]

Hence, these technologies have the capability to gather information without obtaining consent, posing a significant risk to privacy rights because, once private information is exposed, it will result in immeasurable implications.[14] There is no guarantee that the information that is gathered through such extensive monitoring will not be lost, stolen, or misused in any way. In light of the fact that it is obvious that it violates the rights of the general population, the authorization of mass surveillance for a legitimate purpose raises significant concerns. Therefore, it is a possibility that people will avoid particular activities or locations because they are concerned about being monitored, which will have an effect on their personal and social liberties.

VOICE RECOGNITION AND SPEECH RECOGNITION TECHNOLOGY

Voice recognition and speech recognition technology are part of biometric technologies, which utilize distinctive human characteristics associated with physical features such as voice, speech, fingerprints, gait, iris, and retina. Unlike other identifiers such as IP addresses or passwords, these biometric characteristics cannot be lost, destroyed of, or replaced. These are deemed sufficiently stable to be utilized for highly dependable identification.[15] One commonly utilized biometric technology in today's world is voice recognition, which is employed to identify and

[13] ACLU v Clearview AI Inc, No 9337839 (Circuit Court of Cook County, Illinois, 28 May 2020) https://www.aclu.org/cases/aclu-v-clearview-ai

[14] Yang Z and Xu Y, 'Privacy and Data Protection Risks Caused by Artificial Intelligence' (Zhong Lun Law Firm, 29 September 2021) https://www.zhonglun.com/research/articles/8670.html

[15] Roy A, 'Voice Recognition: Risks to Our Privacy' *Forbes Opinion* (6 October 2016) https://www.forbes.com/sites/realspin/2016/10/06/voice-recognition-every-single-day-every-word-you-say/

authenticate an individual's voice. It is primarily used in telephone communication, voice input, and voice search. On the other hand, speech recognition refers to the technology that can convert human speech into machine-readable text. The natural language processing-based speech recognition system collects, understands, translates, and transcribes speech, commonly used in areas such as security authentication and intelligent control systems. Voice recognition and speech recognition technology are closely linked, although speech recognition poses greater technical challenges.

Voice recognition and speech recognition are often used interchangeably, but they serve different functions. In smart home devices and virtual assistants such as Siri and Alexa, voice recognition technology analyzes the command of the household member. If the individual has the necessary access, voice recognition can authenticate their identity. Subsequently, speech recognition converts their spoken commands into text, enabling the device to perform actions such as adjusting the temperature or playing music. YouTube, a popular video platform, utilizes speech recognition to automatically generate captions for video clips. Additionally, voice recognition is employed to ensure that the captions accurately correspond to the speaker's voice. Also, in language learning applications, voice recognition technology is used to analyze the spoken words of the speaker and assess their pronunciation. On the other hand, speech recognition technology evaluates the speaker's fluency and accuracy in the target language.

Based on the studies, the widespread adoption of this technology has led to an increase in security and privacy risks, which is a concerning situation. The market for this technology is expanding rapidly, leading to an increase in market share each year. However, persistent privacy and security concerns continue to result in significant economic losses and pose a threat to users' personal sensitive information. Research has revealed that voice assistants such as Siri or Alexa can be unintentionally activated, making them vulnerable to exploitation by malicious attackers. Possible yet significant threats encompass bank transfers, purchasing virtual goods, forging messages to your intimate acquaintances or relatives soliciting funds, pilfering your credential data, and numerous additional risks. Significant financial and emotional damages can result from the unauthorized access of voice assistant applications.[16] It can easily be attacked as it was found that, the virtual assistant is vulnerable to malicious attacks, similar to other

[16] Li J and others, 'Security and Privacy Problems in Voice Assistant Applications: A Survey' (arXiv, 19 April 2023) https://arxiv.org/pdf/2304.09486

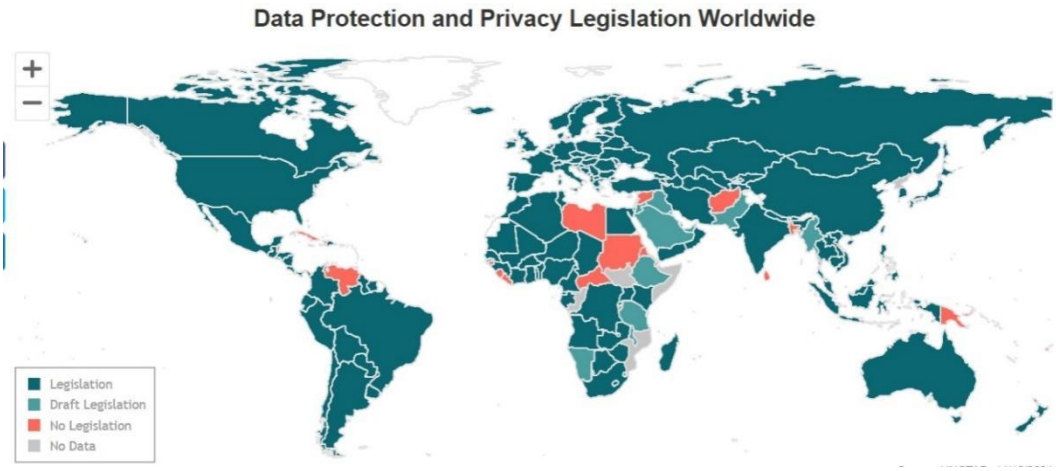
connected gadgets that have been targeted in the past.[17] Therefore, it can be noted that the voice recognition technology itself is not responsible for the issue. The issue pertains to the utilization and safeguarding of these acknowledged voice data. Various companies and institutions employ voice recognition technology to gather and analyze individuals' voice data, including users' phone commands and voice assistant logs. The data is automatically transformed into text format in the background for the purpose of training and utilization by machine learning algorithms. Nevertheless, in the absence of adequate safeguards, it is highly probable that this data will be illicitly acquired and exploited, thereby violating individuals' privacy.[18]

Mass surveillance, facial recognition, speech and voice recognition technologies offer many benefits in terms of efficiency and configuration; nevertheless, they also generate major privacy rights and other human rights issues. For instance, the surveillance system that is based on artificial intelligence collects private data without regard for its privacy. AI technology can enable the collection of data in a non-discriminatory manner and the development of a variety of products that are capable of "indiscriminate surveillance" in a specific region. Also X, formerly Twitter, combined with Grok, an artificial intelligence chatbot, X teaches Grok using user posts; unless users specifically decide not to engage in this process. Users must expressly opt out to prevent their posts from being included; default usage of user data is for AI training. X recently added a provision in its privacy settings that lets users decide not to participate; the precise date of when this function was made available and when data collecting started is yet unknown.[19] Given user data being used without their knowledge, it may be concluded that this method is pervasive in all artificial intelligence technology.

Users willingly accept and benefit from the convenience of artificial intelligence technology, but in doing so, they also expose their personal information to the rapid advancements in artificial intelligence. Once autonomous cars become the prevailing mode of transportation, users will ultimately sacrifice their control over their own privacy and be compelled to share personal information, such as travel patterns and workplace addresses, with car service

[17] Bolton T and others, 'On the Security and Privacy Challenges of Virtual Assistants' (2021) 21(7) *Sensors* 2312.
[18] Rich2021, 'The Development of Speech Recognition and the Challenge of Privacy Protection' (Baidu Developer, 8 October 2023) https://developer.baidu.com/article/details/1919997
[19] Axon S, 'X is Training Grok AI on Your Data—Here's How to Stop It' *Ars Technica* (26 July 2024) https://arstechnica.com/ai/2024/07/x-is-training-grok-ai-on-your-data-heres-how-to-stop-it/

providers. As technology continues to advance and become more widely used, this statement holds particularly true. [20] Similarly, this applies to all other technologies. If we provide our personal information to enhance the efficiency and rapid advancement of artificial intelligence technology, we must relinquish some of our privacy rights. Given the current state of affairs, this is a situation that lawmakers and policymakers should be concerned about. Policymakers are increasingly prioritizing the development of systems that ensure strong protection of individual data privacy. At the same time, individuals highly value the conveniences offered by artificial intelligence. According to the United Nations Conference on Trade and Development (UNCTAD), 71% of countries have enacted legislation aimed at safeguarding data and privacy. Currently, 9% of countries are in the process of creating laws on this topic, while 15% have not yet put any privacy laws into effect. Additionally, 5% of countries have no available information on their legislative status, as indicated in Figure 1.**Figure: 1**[21]



CONCLUSION

The earlier discussion addressed the important methodologies by which artificial intelligence operates, as well as the various applications and the consequential effects on the right to privacy. The incorporation of artificial intelligence (AI) into different fields presents notable advantages, but it also raises substantial privacy concerns. Technologies like AI surveillance, face recognition, voice recognition, and space recognition have the capacity to improve the performance of their respective functions. The use of AI surveillance and facial recognition

[20] Liu Y, 'The Impact of Artificial Intelligence on Privacy Rights and Legal Responses' *People's Forum* (September 2020) http://paper.people.com.cn/rmlt/html/2020-09/11/content_2012543.htm
[21] United Nations Conference on Trade and Development, *Data Protection and Privacy Legislation Worldwide* https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

technology has the potential to enhance security measures, but it also raises concerns regarding privacy, posing risks to personal anonymity and consent. Conversely, voice and speech recognition technology can enhance user interaction and facilitate the usability of AI products. However, it also poses a potential threat in terms of data storage and unauthorized access to personal information, The right to privacy is of utmost importance and highly susceptible in the digital era, as it can be easily compromised, leaving the user unaware of such infringement. The disclosure of private data and information can significantly undermine the right to privacy, as well as other fundamental human rights. Of particular concern is the right to dignity, which is not bound by any legal restrictions and should be respected universally and at all times. In order to establish explicit ethical guidelines and regulations for the development and implementation of AI systems, it is imperative that governments, corporations, and individuals collaborate. This will ensure the preservation of individual liberties and facilitate the effective application of advanced technology.