PROTECTING HUMAN RIGHTS IN THE DIGITAL ERA THROUGH THE USE OF ARTIFICIAL INTELLIGENCE AND PRIVACY

By Gurleen Kaur[*]

ABSTRACT

The intersection of Artificial Intelligence (AI) and privacy in the digital era has significant ramifications for human rights. This article investigates the complex relationship between AI and privacy, analysing ethical factors, legal frameworks, and emergent issues. Developments and the responsibilities of organisations and institutions in protecting individual rights. Beginning with a review of AI technology and its uses, the conversation goes into the definition and significance of privacy in the digital domain. It scrutinises how AI systems utilise personal data, explaining potential privacy dangers and ethical dilemmas. Legal frameworks and international standards governing privacy and AI are addressed, underlining the importance of regulatory compliance and global cooperation. Differential privacy and federated learning are two examples of privacy-preserving AI technologies that are being investigated as ways to protect user privacy in the face of big data proliferation. Transparency, justice, and accountability are among the ethical precepts that underpin AI development and are highlighted as crucial protections against invasions of privacy. In order to preserve privacy as a basic human right in the digital age, this paper promotes an all-encompassing approach to AI governance that is based on moral standards and legal protections.

Keywords: Roles, Awareness, Privacy, Human Rights, and Artificial Intelligence.

[*] Ph.D. Scholar, Sri Guru Granth Sahib World University, Punjab, Email: kgurleen389@gmail.com.

I. Introduction

Artificial intelligence (AI) is at the front of a historic technological revolution, signalling the start of a new era of creativity. However, this revolutionary power also brings with it a maze of privacy issues that go right to the heart of human rights. As AI systems become more and more integrated into everyday life, protecting personal information becomes a crucial concern.

This paper goes extensively into the complicated dance between privacy and artificial intelligence, examining the social, legal, and ethical dimensions that underpin this modern quandary. From the algorithms that predict our next online click to the monitoring systems that follow our locations, the digital era compels us to reconsider the boundaries of privacy. We navigate the challenging area where technology and humans collide by carefully examining the delicate interplay between privacy and artificial intelligence. Join us as we discuss the critical need to find a balance between innovation and the defence of fundamental human rights so that, in the digital age, development does not violate people's right to privacy.

II. Research Methodology

The research employs a qualitative, doctrinal, and comparative approach that draws on academic commentary and source legal texts. In addition to the EU's GDPR and AI Act, it examines international instruments (UDHR, ICCPR), Indian constitutional provisions (Art. 14, 19, 21), significant privacy and surveillance rulings (such as Puttaswamy), and laws like the IT Act 2000 and the Digital Personal Data Protection Act 2023. Books, law-review papers, and policy studies on AI, privacy, and data protection are examples of secondary sources that are utilised to build rights-based suggestions for AI governance and to critically assess current norms.

III. Identification of Statement of the Research Problem

AI-powered biometric, profiling, and surveillance technologies have increased the extent and opacity of personal data usage, threatening autonomy, equality, privacy, and dignity. Significant gaps exist in enforcement and protection due to the present human AI-specific damages aren't protected by Indian constitutional and privacy frameworks, including Puttaswamy and the DPDP Act 2023. This paper proposes doctrinal, legal, and technological modifications to ensure that AI development and implementation remain consistent with a robust right to privacy. It also looks into whether current international and Indian legal frameworks adequately safeguard human rights in the face of AI.

IV. Analysis and Findings of the Research

A. *The Role of Artificial Intelligence in Modern Society*

"The science of giving machines human intelligence is known as artificial intelligence."[1] One of the branch of computer science known as artificial intelligence seeks to replicate human thought and learning. The study of artificial intelligence (AI) aims to build intelligent computers that are capable of all the activities that call for human intellect, including speech and voice recognition, natural language comprehension, and decision-making. To put it simply, artificial intelligence (AI) systems are machines that can perform certain tasks that the human brain can, indicating that they have cognitive capabilities.[2]

A few fundamental and primary approaches that are used to produce intelligent behavior in machines are listed below. Artificial Intelligence (AI) is a collection of several techniques. A branch of computer science called "machine learning" creates algorithms that learn from experience and get better over time.[3] It is an artificial intelligence (AI) subtype that gains knowledge from combined data and gradually becomes better at what it does. Put more simply, it's a technique for giving a machine human-like thought processes. Machine learning algorithms, for instance, are employed to mimic human abilities like driving, playing games, annotating images, and so on.

1. Natural Language Processing (NLP): NLP is a branch of artificial intelligence (AI) and computer science that employs machine learning to assist computers in comprehending and communicating in human language.[4] Prediction and language translation NLP is used by well-known websites like Google to translate and grammatically correct sentences. Natural Language Processing (NLP) is used by virtual assistants like Siri and Alexa to understand, receive, and respond to human commands. Like Gmail, Natural Language Processing (NLP) is used as an email filter to filter spam and accurately categorise emails into main, social, and promotional groups.
2. Robotics: Artificial intelligence for movement is made possible by robotics. These are artificially intelligent devices that can carry out tasks that typically call for human intellect

[1] McCarthy, J. (2007). What is artificial intelligence? Stanford University. http://www-formal.stanford.edu/jmc/visted on 2 November,2025.

[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.

[4] IBM, 'What is NLP (Natural Language Processing)?' (no date) https://www.ibm.com/topics/natural-language processing accessed on 2 November 2025.

both fully and partially on their own. 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 are just a few of the robotic applications that can benefit from the use of AI technologies. The many components of artificial intelligence (AI), such as machine vision, pattern recognition, autonomous navigation, voice recognition, precision manipulation, localisation, and mapping, all play crucial roles. Basic features of sophisticated artificial intelligence, such learning from prior experiences and forecasting the outcome of a certain action, improve these operations.[5] Although artificial intelligence offers crucial opportunities to leverage and apply to create great results in a number of industries, including healthcare, education, and finance, among others, it also poses major risks that should not be disregarded.

B. *Understanding The Right to Privacy*

"The right that determines the nonintervention of secret surveillance and the protection of an individual's information" is the legal definition and definition of privacy.[6]Simply put, the right to privacy prohibits someone from becoming the target of unwelcome exposure. Information privacy, body privacy, communications privacy, and territory privacy are some of the several aspects that make up 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".

Examining the UDHR and ICCPR's aforementioned provisions, we can conclude that they are appropriate for the days of telegrams and paper records, when the digital and technological

[5] Bogue R, 'The Role of Artificial Intelligence in Robotics' (2014) 41(2) Industrial Robot 119.

[6] The Law Dictionary, 'Privacy' (2.11.2025) https://thelawdictionary.org/privacy.

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

revolution was unthinkable. However, times have changed and technology has become more prevalent in society. Under these laws, it is challenging to establish the limits and boundaries of the right to privacy.

The provisions outlined in earlier human rights treaties and conventions are no longer seen as appropriate in light of this technological transformation. Individuals and even states are now included in the expanded definition of privacy. The expansion of privacy rights is facilitated by a variety of practices, including surveillance, data gathering, data analysis, profiling, facial recognition technologies, voice and biometric data, and more. Since technology is changing every day in the digital age, there is a need for a more thorough understanding of privacy. To give a thorough understanding of the right to privacy that is applicable to different historical eras, Solove divided privacy into six different categories.

- The right to be left alone and not to be bothered.
- Limited access to the self, protecting the safety of one's personal information, preventing unauthorised access or disclosure.
- Secrecy, the deliberate practice of hiding certain information or concerns from others.
- Control over personal information, the capacity to exercise authority over personal information.
- Personhood, the preservation of ones' personality, individuality and dignity and;
- Intimacy, exercising authority or imposing limits on one's personal relationships or parts of life.[8]

C. *AI Applications And Their Impact On Privacy Rights*

In artificial intelligence, data is gathered to improve the system's effectiveness, accuracy, and efficiency. When there is more and better quality user data accessible, artificial intelligence systems are better at learning from data and achieving better results.[9]However, the use of AI in many facets of contemporary life may have an effect on the basic right to privacy, which in turn may have an effect on the right to dignity.

Artificial intelligence has drastically changed industrial labor, opened up new avenues for innovation, and improved upon existing ones. However, issues related to AI are becoming more and more serious every day, which presents a worrying challenge for the present day. Biases, a

[8] Solve DJ, Understanding Privacy (Harvard University Press 2010).

[9] Bartneck C and others, 'Privacy Issues of AI' in SpringerBriefs in Ethics (Springer 2020) 61–70.

lack of impartiality, unemployment, and privacy concerns are some of the problems that come with integrating AI.

D. *Legal Framework On AI And Privacy*

1. *Human Rights and Constitutional Framework:* International: Article 12 of the UDHR and Article 17 of the ICCPR regarding arbitrary interference with privacy, honour, and reputation.
2. The Indian Constitution: Article 21: The foundation for privacy, informational self-determination, and dignity is the right to life and personal liberty. Article 14: protection against the arbitrary and discriminatory application of AI technologies, particularly in automated decision-making and profiling. Article 19: Consequences of widespread AI surveillance for freedom of speech and association.
3. Technology and Data Protection Laws: Digital Personal Data Protection Act 2023: specific sensitivity of biometric and other personal data utilised in AI systems; consent requirements; purpose limitation; data minimisation; obligations of data fiduciaries; fines for violations. The IT Act of 2000 and its regulations on electronic records, intermediaries, and appropriate security standards; its limitations in addressing problems unique to artificial intelligence, such as algorithmic opacity and profiling. EU GDPR: as a comparable gold standard, legal foundations for processing, data subject rights (access, correction, deletion, objection), and safeguards against purely automated decision-making (Article 22). New AI-specific laws as normative guidelines for India, such as the EU AI Act 2023 (risk-based categorisation, prohibitions on certain AI applications, tighter controls for high-risk systems).

E. *AI Surveillance And Facial Recognition*

The French term “surveillance,” which means “watching over,” is where the phrase originates? Simply put, surveillance is the process of keeping an eye on and observing a person or group of people in order to provide care and control. Thus, AI surveillance is the application of artificial intelligence technology to watch and evaluate human behavior for a variety of purposes, such as marketing, law enforcement, security, and even keeping an eye on people's emotional states in public areas. Big data in analytical applications is now much less expensive thanks to the internet and artificial intelligence. These days, cameras are present in every aspect of our everyday lives. Every action we take while walking the streets is continuously tracked by AI surveillance, and there is no way for people to avoid the ongoing gathering of personal data.

The strategy involves analysing enormous amounts of data and looking for trends or anomalies in human behavior using complex algorithms and machine learning techniques. Using visual data gathering and analysis techniques, the surveillance footage is examined in real-time to identify items of interest, discover abnormalities, and recognise faces. Artificial Intelligence and reliable information management in government health. Monitoring is effective in the measurement of widespread infectious diseases, in prediction of trends and support of interventions by the public health in managing diseases. It is also training on future medical emergencies. The system assists in crime prevention by observing suspicious movements and enhancing security and safety of the public areas by the use of the artificial intelligence (AI)-assisted technology in the security and safety surveillance.

In the ACLU v. Clearview AI case, Clearview AI, a company, collected around 3 billion faceprints from publicly accessible images, which were then utilised 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 Clear view services throughout the United States. Additionally, the court barred them from providing face print databases to any entity in Illinois, including state and local police, for a period of five years.[10]

As a result, these technologies have the capacity to collect data without authorisation, which poses a serious threat to people's right to privacy because the consequences of disclosing personal information are enormous.[11]There is no assurance that the data collected by such thorough surveillance won't be misplaced, stolen, or used improperly. The authorisation of mass monitoring for a lawful reason raises serious problems since it is evident that it infringes the rights of the general public. As a result, people may steer clear of specific activities or

[10] 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.

[11] 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

places out of fear of being watched, which might have an impact on their social and personal freedoms.

F. *Voice Recognition And Speech Recognition Technology*

Biometric technologies, which use unique human traits linked to physical attributes like voice, speech, fingerprints, gait, iris, and retina, include voice and speech recognition systems. These biometric traits cannot be lost, destroyed, or changed, in contrast to other identifiers like IP addresses or passwords. These are thought to be stable enough to be used for extremely reliable identification.[12] Voice recognition is one biometric technique that is frequently used in today's world to identify and authenticate a person's voice. Voice input, voice search, and telephone conversation are its main uses. Conversely, the technology that translates human voice into machine-readable text is known as speech recognition. The method based on natural language processing Speech recognition systems, which are frequently utilised in fields like intelligent control systems and secure authentication, gather, comprehend, translate, and transcribe speech. Although speech recognition has more technical difficulties, voice recognition and speech recognition technologies are closely related.

Voice recognition and speech recognition are often used interchangeably, but they serve different functions. Voice recognition technology evaluates a household member's command in smart home appliances and virtual assistants like Siri and Alexa. If the individual hasthe necessary access, voice recognition can authenticate their identity. The device can then carry out tasks like playing music or changing the temperature thanks to speech recognition, which translates their spoken commands into text. YouTube, a well-known video website, automatically creates subtitles for video recordings using voice recognition. Furthermore, speech recognition is used to guarantee that the captions precisely match the speaker's voice.

According to the research, there are now more security and privacy threats as a result of this technology's broad use, which is alarming. This technology's market is growing quickly, increasing its market share annually. However, ongoing privacy and security issues continue to cause large financial losses and endanger users' sensitive personal data. According to research, voice assistants like Siri and Alexa can be accidentally enabled, leaving them open to abuse by

[12] 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 .

malevolent hackers. Bank transfers, buying virtual products, faking communications to your close friends or family members requesting money, stealing your login credentials, and many more concerns are all potential but serious threats. Unauthorised access to voice assistant programs can cause serious financial and psychological harm.[13]

Similar to other connected devices that have previously been targeted, it was discovered that the virtual assistant is susceptible to malicious assaults.[14] Thus, it should be underlined that the problem is not caused by speech recognition technology per such. The use and protection of this recognised voice data are at dispute. Voice recognition technology is used by many businesses and organisations to collect and examine voice data from people, including phone instructions and voice assistant records. In order to train and use machine learning algorithms, the data is automatically converted into text format in the background. However, it is very likely that this data will be illegally obtained and used, compromising people's privacy, in the lack of sufficient protections.[15]

While facial recognition, speech, and voice recognition technologies, as well as mass monitoring, have numerous advantages in terms of efficiency and setup, they also raise significant privacy rights and other human rights concerns. For example, the artificial intelligence-based monitoring system gathers personal information without considering its privacy. AI technology can make it possible to gather data in a non-discriminatory way and create a range of devices that can do "indiscriminate surveillance" in a certain area. Additionally, Grok, an AI chatbot, is trained by X, the former Twitter, using user contributions, unless users expressly choose not to participate. Users' postings cannot be included unless they specifically opt out; by default, user data is used for AI training. X recently introduced a feature in its privacy settings that allows users to choose not to participate; it's unclear exactly when this feature became accessible and when data collection began.[16]It may be inferred that this technique is ubiquitous in all artificial intelligence technologies as user data is utilised without the users' awareness.

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

[14] Bolton T and others, 'On the Security and Privacy Challenges of Virtual Assistants' (2021) 21(7) Sensors 2312.

[15] Rich2021, 'The Development of Speech Recognition and the Challenge of Privacy Protection' (Baidu Developer, 8 October 2023) https://developer.baidu.com/article/details/1919997

[16] 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/

Users voluntarily embrace and profit from artificial intelligence technology, but by doing so, they expose their personal data to the swift progress of AI. When driverless vehicles take over as the most common form of transportation, consumers will eventually give up control over their privacy and be forced to provide car services access to personal data like company addresses and travel schedules. suppliers. This is especially true when technology develops and spreads.[17]This also holds true for every other technology. We must give up part of our privacy rights if we give our personal information to improve the effectiveness and quick development of artificial intelligence technologies. Legislators and politicians ought to be concerned about this given the current scenario. The creation of systems that guarantee robust protection of individual data privacy is becoming a top priority for policymakers.

G. *Case Analysis*

1. Justice K.S. Puttaswamy (Retd.) v. Union of India[18]

   In Justice K.S. Puttaswamy (Retd.) v. Union of India, a nine-judge Bench of the Supreme Court unanimously recognised the right to privacy as a fundamental right under Article 21, intrinsically connected with dignity, autonomy, and informational self-determination. The Court laid down that any intrusion into privacy must satisfy a four-fold test of legality, legitimate aim, necessity, and proportionality, alongside procedural safeguards, which now forms the constitutional standard for evaluating AI-enabled surveillance, profiling, and data processing.

2. K.S. Puttaswamy v. Union of India (Aadhaar)[19]

   In the Aadhaar judgment, the Supreme Court upheld the core of the Aadhaar scheme but imposed strict limits on the collection and use of biometric data, emphasising purpose limitation and the dangers of creating an architecture of surveillance. The Court's concerns about function creep and centralised biometric databases are directly relevant to large-scale facial recognition and AI-driven identification systems that rely on continuous data aggregation.

[17] 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

[18] (2017) 10 SCC 1.

[19] (2019) 1 SCC 1.

3. R. Rajagopal v. State of Tamil Nadu.[20]

   In R. Rajagopal v. State of Tamil Nadu, the Supreme Court affirmed that the State cannot publish or authorise publication of details of a person's private life without consent, recognising a right to be let alone as part of Article 21. This early articulation of informational privacy supports the view that indiscriminate AI-based surveillance and profiling without legal backing or consent violates the protected sphere of private life.

H. *A Path Forward: Mitigating AI's Privacy Risks*

AI poses serious privacy issues, but they are manageable. A proactive, multi-stakeholder approach is required to optimise AI's benefits while upholding fundamental human rights. The following pillars create a comprehensive roadmap for a more privacy-conscious digital future.

1. Strengthening the law and regulatory frameworks: The existing system of law is not usually up to date with the technological progress. We suggest the following actions to this: Principle-Based law: Rather than industry-specific rules, governments must enact comprehensive, principle-based AI governance law. Laws like the EU's AI Act, which groups AI systems in accordance to risk and places stringent restrictions on high-risk uses. Lawmakers should mandate "Privacy by Design" and "Data Protection by Default" for AI systems. This suggests that privacy protection is an essential component rather than a consideration, ensuring that systems have the greatest privacy settings by default and collect only the necessary data.

2. Developing Technological Protections: Technology itself may hold the key to this problem. We really need to work on creating and using methods, for Privacy-Preserving AI or PPAI for short and actually put these methods into practice. This is important for Privacy-Preserving AI techniques to be effective. Developing and using Privacy- AI techniques is crucial.

   - *Federated Learning*: This method uses local data to train AI models across several decentralised devices (such as smartphones) without ever sending the raw data to a central server. This provides individuals more control and reduces the possibility of significant data breaches.
   - *Differential Privacy*: This mathematical framework guarantees that no individual's information will be revealed in the analysis's result while also enabling computers to

[20] (1994) 6 SCC 632.

learn from massive datasets. It operates by deliberately adding a certain quantity of "statistical noise."

3. Promoting Corporate Accountability and Ethical Governance
   - Regulators should be able to access the results of these audits, which should assess systems for bias, fairness, openness, and privacy compliance.
   - Explainability and Transparency (XAI): "Explainable AI" (XAI) has to be promoted. When an AI system makes a decision that impacts a person's rights, such as rejecting a loan or screening a job application, the person has a right to a comprehensible explanation of the reasoning that went into that decision. In doing so, "black box" algorithms are abandoned.

I. *Encouraging People via Literacy and Public Awareness*

Lastly, people cannot defend rights they are unaware of.

1. *Digital Literacy Initiatives*: Data and digital literacy must be included into public education by governments and educational establishments. People must be aware of their rights and how their data is gathered, utilised, and valued.
2. *Accessible Tools and Settings*: It is the duty of IT businesses to give consumers easy-to-use, transparent privacy settings. As X ultimately made available, settings to opt out of data collecting for AI training should be visible and simple to locate by default, rather being hidden under intricate menus. We can build an environment where artificial intelligence benefits mankind without jeopardising the basic right to privacy by combining these four pillars: strong legislation, cutting-edge technology, moral business conduct, and an empowered public.

V. Conclusion

The preceding discussion addressed the vital mechanisms by which artificial intelligence operates, its wide range of applications, and the consequent consequences for the right to privacy. While incorporating artificial intelligence (AI) into a variety of industries has obvious advantages, there are also serious privacy issues. AI surveillance, face recognition, voice recognition, and spatial recognition are examples of technologies that can enhance the effectiveness of their respective roles. AI applications for facial recognition and surveillance.Technology can improve security measures, but it also creates privacy issues and puts consent and personal anonymity at danger. On the other hand, voice and speech recognition technologies can improve user engagement and make AI products easier to use. But it also presents a risk for data storage and illegal access to personal data. In the digital age, the right to privacy is crucial and extremely vulnerable as it may be readily violated without the user's knowledge.

The right to dignity, which is unconstrained by law and should be upheld everywhere and at all times, may be gravely jeopardised by the disclosure of personal information that is very relevant. Governments, corporations, and individuals must collaborate to establish unambiguous moral guidelines and legal requirements for the development and use of AI systems. This will enable the effective use of cutting-edge technology and ensure the protection of individual liberties.

****