

Artificial Intelligence and Humans: Assessing the Effects on Privacy and Freedom

OPEN ACCESS

Manuscript ID:
ASH-2024-12028011

Volume: 12

Issue: 2

Month: October

Year: 2024

P-ISSN: 2321-788X

E-ISSN: 2582-0397

Received: 22.08.2024

Accepted: 29.09.2024

Published Online: 01.10.2024

Citation:

Joseph, Binu. "Artificial Intelligence and Humans: Assessing the Effects on Privacy and Freedom." *Shanlax International Journal of Arts, Science and Humanities*, vol. 12, no. 2, 2024, pp. 127–37.

DOI:


<https://doi.org/10.34293/sijash.v12i2.8011>



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

Binu Joseph

Assistant Professor, NA Global Law School, Bangalore, Karnataka, India

 <https://orcid.org/0000-0001-7582-3499>

Abstract

Artificial Intelligence (AI) is a multidisciplinary area that integrates elements from several domains. Sometimes, it is also called deep learning or machine learning. And it can simply be referred to as making machines capable of thinking like humans and acting like humans. The process of AI involves developing specific algorithms in order to solve complex tasks that are difficult for humans. With the advancement of innovative technologies, the role of machines has become an inevitable factor in almost all fields of human life. AI has emerged as a super-intelligent mechanism that can solve many issues and find solutions suddenly and promptly. However, such an application of AI has also created numerous challenges against human rights. The greatest threat posed by the use of AI is the infringement of individual freedom and privacy. AI has now enabled the management of many human activities, and this management has led to excessive control of machines over human affairs. AI can gain access to individuals' personal lives without their consent. Data protection is another challenge of AI, as it can violate individuals' privacy and freedom. The detractors of AI argue that it has no respect for individuals' emotions and social values because most of the AI is generated through such algorithms. This paper discusses how AI impacts human activities by compromising individuals' privacy and freedom. Similarly, it discusses AI regulatory mechanisms that have been taken at national and global levels. Furthermore, it provides key recommendations in order to regulate the excess interference of AI technology over human affairs.

Keywords: Artificial Intelligence, Human Rights, Freedom, Privacy, Technology

Introduction

The contemporary era is significantly influenced by the use of machines and digital technology. With the advancement of science and technology, the modern era is going through the timeline of the fourth industrial revolution, wherein machines stand as an inevitable factor in managing human activities. The technology has further advanced into the age of Artificial Intelligence (AI). AI is a subfield of computer science, and it is concerned with building machines that can carry out operations that normally require human intelligence. The term AI was first used by John McCarthy in 1956. He was an American computer scientist, and he used the term AI in a research proposal for the Dartmouth Conference. In a simple way, AI can be defined as a machine or system that can accomplish any task that a human can perform. In a recent Stanford University report, AI is defined as 'a science and a set of computational technologies that are inspired by but typically operate quite differently from the ways people use their nervous systems and bodies to sense, learn, reason, and take action' (Stanford University). Jootaek Lee opined 'AI is a computer machine with the ability to make predictions about the future and solve complex tasks, using algorithms' (Lee). The specified algorithm setting enables AI to perform human-like intelligence and solve complex tasks. The term 'algorithm' is commonly used in the fields of big data, machine learning, and artificial intelligence.

An algorithm is a set of commands that allow a computer to change an input into an output (European Union Agency for Fundamental Rights). For example, a list of people has to be sorted by age. The computer takes the ages of the persons on the list (input) and generates a new ranking (output). AI is also a mix of terms such as big data, machine learning, or deep learning, and they have in common the analysis of large centralised data using costly computer power. AI is enabled to solve tasks such as learning, problem-solving, interacting, perception, learning, reasoning, and language understanding. The goal of Artificial Intelligence (AI) is to create machines that can emulate human cognitive processes by thinking, learning, and adapting. AI is also encompassed by a vast array of methodologies and techniques, and it draws from the disciplines of computer science, big data, engineering, data science, engineering, cognitive science, mathematics, applied mathematics, and philosophy (AUDA-NEPAD). Many countries in the world have already benefited from the progress of AI. Notably, countries such as the US, China, Japan, France, and the UK, with their significant skilled human capital, are global leaders in AI. For instance, China and the United Kingdom project that by 2030, AI-related businesses and activities will account for 26% and 10% of their GDPs, respectively (NITI Aayog).

Nowadays, AI machines have begun to perform the jobs that humans had done earlier. In many fields, machines have already replaced humans' labour potential. However, enabling machines to be capable of human intelligence has many drawbacks. The incorporation of AI technologies into various industries has prompted various concerns. And these concerns are multidimensional, encompassing legal, ethical, and technological elements. Some major concerns are data security, data anonymization, data minimization, regulatory compliance, bias, transparency, and accountability. Besides, the interaction between AI and humans creates substantial risks, mainly relating to their privacy and freedom. The risks that AI creates for individual freedom are generally related to AI-powered monitoring and surveillance, individual decision-making, autonomy, and freedom of expression. Similarly, AI may risk the privacy of individuals through data collection,

storage, usage, and sharing. And such risks have created enormous concern among people relating to the use of AI in day-to-day affairs. Besides, many countries are now cautious about the excess interference of AI in human affairs. Hence, many countries have already implemented a number of legal and administrative frameworks to regulate AI technologies and protect individuals' privacy and freedom.

AI and Humans

Humans' innovations have shaped their lives in different ways. In this era, humans find it challenging to survive without the support of machines and technologies. Machines have been controlling their lives in one way or another. After the emergence of AI technologies, most of their efforts have been transferred to machines. The advancement of AI technologies has immensely benefitted humans' day-to-day lives. In most of the areas, especially education, healthcare, transportation, cybersecurity, scientific research, and entertainment, the use of AI has brought tremendous transformations. And all these changes have benefitted humans in a way of speedy and promptly accessing information and providing results. For instance, Hanson Robotics has developed a humanoid robot named Sophia with the capability to take part in interviews and later obtain Saudi Arabian citizenship. Sophia Humanoid became the first-ever Innovation Champion of the United Nations Development Programme (UNDP), becoming the first non-human to hold such a designation. Jeff Bezos, the founder, and CEO of Amazon, has adopted a robotic dog named Spot Mini, who can open doors, get up on his own, and even load the dishwasher. Likewise, AI technologies have been used in many areas for the well-being of humans.

AI on Individual Privacy and Freedom

AI and individual privacy and freedom interact in a complicated way that offers both major advantages and substantial risks. For an individual, the essential basic rights are privacy and freedom. Article 12 of the Universal Declaration of Human Rights says 'No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to

attacks upon his honour and reputation, and everyone has the right to the protection of the law against such interference or attacks’ (Universal Declaration of Human Rights). Furthermore, the International Covenant on Civil and Political Rights specified in its Article 17 that ‘no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence, nor unlawful attacks on his or her honour and reputation’; ‘everyone has the right to the protection of the law against such interference or attacks’ (International Covenant on Civil and Political Rights). Similarly, privacy is a comprehensive concept that encompasses the development and understanding of humanistic, anthropological, and sociocultural values through various cognitive and systemic approaches (Abhivardhan). Similarly, freedom also encompasses distinctive ideals of speech, expression, assembly, movement, employment, etc. In the modern era, all jurisprudences have given special attention to the protection of individual privacy and freedom, because these are fundamental for an individual’s self-development. With the advancement of innovative technologies, individuals are directly or indirectly under the control of such technologies. Likewise, human beings have been subjugated or depended upon technologies to manage their daily lives. In such a circumstance, individual privacy and freedom are compromised by technology. AI is also such a technology that can manage and control an individual’s personal affairs directly or indirectly.

AI technologies can create numerous challenges to the existence of humans, especially with regard to human rights. The following human rights are also pertinent to AI: equality before the law, privacy, data protection, freedom of speech, and fair access to necessities (such as healthcare) (WHO). For AI systems to perform better and train their algorithms, large amounts of data are frequently used. According to the EU Agency for Fundamental Rights, ‘an algorithm never returns a definitive result only probabilities’ (European Union Agency for Fundamental Rights: *Facial Recognition Technology*). The setting of AI algorithms is often complex and provides complicated information because their neural network has an input layer, an output layer, and several hidden layers of artificial

neurons (Zornetta and Cofone). This is referred to as the black box phenomena due to the challenge in comprehending how the outcome is achieved when data is processed through the network (Zornetta and Cofone). It will also create concerns about AI transparency and accountability. Personal information like names, addresses, and financial data, as well as sensitive data like social security numbers and medical records, might all be included in this data. Concerns over its use and accessibility may arise from the gathering and processing of this data (The Economic Times). Since the processing of personal data may put fundamental rights and freedoms in danger, those rights and freedoms should receive special protection. Personal data are, by their very nature, especially sensitive to these issues (European Parliament & Council of the European Union). AI technology can assist in the encrypting, organisation, compression, and duplication of an individual’s data into data storage. These personal data are often necessitated by the government and other public authorities to identify an individual for many official purposes. AI systems come with inherent risks, like compromised privacy, entrenched and codified biases, decreased accountability, and increased information asymmetry between system developers, consumers, and lawmakers (MeitY). The application of AI technology in multiple ways can intrude into individuals’ private affairs by breaching their privacy and freedom. AI systems rely on massive amounts of data, which can be exploited by hackers if not adequately protected. Breaches can result in unauthorised access to sensitive data, such as financial records, research data, or personal information. Adversarial attacks manipulate the behaviour of AI models by exploiting weaknesses. Attackers can trick AI systems into providing incorrect findings or judgements by quietly modifying input data (WSU). Regarding crucial industries like autonomous vehicles or medical diagnosis, hostile attacks might be highly concerning. The integrity and usefulness of AI systems can be jeopardised if attackers input dangerous data or secretly alter current data (WSU). This could lead to unfair results, unauthorised access, or service outages. Such a method of manipulating training data to train AI models is known as model poisoning. Privacy is

also a risk in using AI because AI systems typically process large amounts of personal data, which raises privacy concerns. Maliciously, AI technology can also be applied. Malicious applications of AI technology include creating realistic deep fake content, automating social engineering methods, and designing highly complex phishing attack (WSU). The lack of AI transparency in many AI models, such as deep learning neural networks, can create complications and challenges to understanding. Due to a lack of transparency, it is difficult to understand how AI systems make decisions or identify the causes of biases or errors, which may limit accountability and make it more difficult to detect harmful activities (WSU). AI has the ability to automate and enhance social engineering attacks (WSU). Adversaries may manipulate others into giving them unauthorised access to networks or revealing private information. For example, AI-powered voice assistants and chatbots can be created to deceive consumers, enhancing the sophistication of social engineering attacks. Furthermore, in many fields, AI technologies have already been implemented, and using these technologies poses challenges to human privacy and freedom through the means of surveillance, data collection, and breaches, as well as restricting freedom of speech and expression over human beings.

AI technologies can intrude into individual affairs of privacy and freedom in the following ways:

Surveillance

The purpose of using AI in surveillance is to observe and monitor the activities of humans and others. AI in surveillance systems has transformed our understanding of security by improving threat identification, monitoring capabilities, and response systems (Chirag). Various countries are using AI technology to achieve a wide range of surveillance objectives. According to the Artificial Intelligence Global Surveillance (AIGS) Index, across the world, at least 75 of the 176 countries are actively employing AI technologies for surveillance, and it comprises face recognition systems in 64 nations, smart policing in 52, and smart city/safe city platforms in 56 countries (Feldstein). Among these countries, China and the USA are the significant players in using the AI surveillance industry and exporting AI-based technologies to at least 60 other countries (Chirag). The leading AI surveillance supplying technology companies are Huawei, Dahua Hikvision, ZTE (China), NEC Corporation (Japan), IBM, Palantir, and Cisco (USA), and among these companies, Huawei, IBM, and Cisco are the three top suppliers of AI technologies to other countries (Feldstein).

Summary of AI Surveillance Techniques and Global Prevalence

AI Surveillance Technique	Description	Global Proliferation (out of 75 countries)
Smart Cities / Safe Cities	Cities equipped with sensors that broadcast real-time data to improve service delivery, management, and public safety. Sensors and facial recognition cameras are used in these 'safe cities', as they are commonly referred to. Police body cameras are linked to intelligent command centres to help prevent crime, protect public safety, and respond to emergencies. The index includes only platforms that clearly focus on public safety.	56 countries
Facial Recognition Systems	Biometric technology employs cameras (still or video) to compare recorded or live footage of individuals to photos from databases. Not all systems rely on database matching; some systems examine aggregate demographic trends or undertake broader sentiment analysis using facial recognition crowd scanning.	64 countries
Smart Policing	Data-driven analytic technology is used to facilitate investigations and police responses; some systems incorporate algorithmic analysis to make predictions about future crimes.	53 countries

Source: AIGS Index (Feldstein)

However, AI tools that follow people's movements and activities without their permission, such as facial recognition and data analysis, can be utilised for widespread individual surveillance. In public and private settings, this may result in a loss of anonymity and privacy. People may become fearful and self-censor as a result of this widespread surveillance, changing their behaviour since they are aware that they are being observed all the time. Individual freedoms may be compromised by facial recognition. Facial recognition is a biometric technology that utilises cameras, including both video and still images, to compare recorded or real-time footage of individuals with images from a database, though not all systems prioritise individual identification; some are specifically developed to evaluate overarching demographic patterns or perform more comprehensive sentiment analysis by scanning a crowd (Feldstein). By the use of AI technology, we can measure, analyse, identify, and classify people's faces. However, these techniques may also be used to monitor and profile individuals. It is already being utilised in public places like train stations, airports, and other places, as well as by law enforcement. Facial recognition technology is primarily creating two concerns: firstly, there are not many guidelines governing picture database use and access, and secondly, there is a considerable variation in the accuracy of facial recognition technologies (Feldstein). For example, Axon is a leading company that supplies police body cameras in the USA, and it announced ceasing providing face recognition on its devices. The company's independent ethics board stated that 'face recognition technology is not currently reliable enough to ethically justify its use' (Warzel). Facial recognition technology may identify a person's ethnicity, race, national origin, gender, and other features, potentially leading to unlawful discrimination. For example, the Chinese government uses face recognition technology and surveillance cameras around the country to seek for Uighurs (a Turkic ethnic group that mostly lives in the Xinjiang Uyghur Autonomous Region of northwest China) based on their appearance and retains records of their comings and goings for search and inspection (Mozur). Studies carried out on various facial recognition systems (such as

IBM Watson, Microsoft Cognitive Services, and Face++) have demonstrated that certain ethnic groups receive less accurate treatment than others. When face recognition technology is used on women and people of colour, the mistake rate is greater, resulting in biased findings and potentially discriminatory outcomes. Furthermore, facial recognition technology has proven unsuccessful in overcoming persistent gender and racial prejudices, resulting in increased false positives for minorities and women (Feldstein). Interestingly, 99% of Caucasian men were correctly identified, compared to just 34% of women with darker skin tones (Cataleta). This is a result of the algorithms in these systems being built on subject-data inputs that are primarily light-skinned men. There are concerns regarding the influence of AI on employment, the possibility of worker monitoring, and the widespread exploitation of the majority of persons by businesses that can harness the powers of AI (Stahl et al.). In many places, AI-enabled technology is being used to monitor illegal activities and detect wrongdoers. Many individual privacy violations have been reported after the installation of AI cameras in public places. For example, in the Indian state of Kerala, the Kerala Motor Vehicles Department (MVD) has installed AI-enabled surveillance cameras across the state to detect violations of traffic rules. However, it has hailed many criticisms of violating individual privacy by monitoring the movement of citizens. AI can also be used to monitor social media. With the assistance of AI-driven technology, Social Media Monitoring (SMM) software has been developed in order to collect and analyse publicly available data from social media networks. SMM software may identify complex information about a person's identity, current activities, and future objectives (Golunova). For example, Law enforcement officials use SMM software, created by the Israeli company Zency, to generate reports based on information gathered from thousands of social media profiles and organisations (Golunova). Companies, such as data mining corporations and research institutions, develop and promote AI-driven solutions, claiming their discoveries may revolutionize the identification and investigation of illegal acts; however, many of these technologies are opaque, have low accuracy

rates, and may perpetuate biased behaviours (Golunova). Likewise, in many ways, AI technology can interfere with individuals' private affairs and manipulate their decision-making choices.

Restriction on Freedom of Speech and Expression

It is an essential political right of an individual to freely speak and express their opinions. However, with the application of AI technology, the user can manipulate and restrict the individual's freedom of speech and expression. AI advancements enable governments to filter content more precisely, decreasing public backlash and political costs for those in power (Funk et al.). According to the AIGS Index, compared to liberal democracies, governments in autocratic and semi-autocratic countries are more likely to misuse AI surveillance; for instance, governments with poor human rights records, such as Saudi Arabia, China, and Russia, are abusing AI technology for widespread surveillance, while others use it more sparingly to sustain oppression (Feldstein). It is also applied to manipulate information by creating disinformation. AI-based technologies that can create text, audio, and images have rapidly evolved to be more powerful, accessible, and user-friendly, promoting a worrisome spread of these disinformation strategies. AI-generated misinformation is becoming increasingly difficult for observers, moderators, and regulators to detect and delete due to its high quality and quantity. For political motives, AI technology has been used to propagate misinformation in order to target the opponent against their political gains. For example, During the February 2023 Nigerian elections, an AI-manipulated audio tape circulated on social media, accusing an opposition presidential candidate of rigging ballots. AI-generated content was being used in the U.S. to attack electoral opponents. Accounts linked to Donald Trump and Ron DeSantis, both running for the Republican nomination in 2024, shared videos with fake images to damage each other's campaigns. One video showed fabricated images of Trump hugging Dr. Anthony Fauci, who is disliked by many critics of COVID-19 measures. In February 2023, another incident also happened in the US with a fake video claiming President Biden made transphobic comments that went viral on

social media. It was likely intended to harm Biden's reputation among supporters of transgender rights. According to the Freedom on Net 2013 report, in 47 countries where pro-government commentators influence online debates, and in 16 countries, AI-based systems that may produce pictures, text, or audio were utilised to misrepresent information on political or social issues (Funk et al.). These practices can harm public faith in democratic processes, encourage self-censorship among activists and journalists, and prevent accurate and impartial reporting (Funk et al.). AI systems are also capable of acting independently when they form decisions about people in ways that their recipients are unaware of and hence are unable to challenge. (Stahl et al.). Such automatic decision-making capability of AI would curtail the independent choice of individuals. AI technology monitors political activities such as protests, movements, and strikes in public spaces. The right to protest or express dissenting views is also a part of democratic political right. The use of such a mass surveillance apparatus may potentially limit the rights to free assembly and association by preventing individuals from exercising such rights for fear of being targeted or penalised in some way (González). In many places in the world, facial recognition technology already being used to monitoring the protectors. For example, in Russia, activist Alyona Popova lodged a complaint to European Court of Human Rights against the Russian authorities about the use of Facial recognition technology to monitor the protestors (González). Likewise, so many examples can be seen around the world relating to the misuse of AI technology against the infringement of freedom of individuals.

Data Collection and Data Breach

Privacy and data protection are inextricably interconnected. Article 14(1) of the European Union's General Data Protection Regulation (GDPR) defined, 'data subjects are identifiable if they can be directly or indirectly identified, particularly by reference to an identifier such as a name, identification number, location data, online identifier, or specific characteristics expressing the physical, physiological, genetic, mental, commercial, cultural, or social identity of these natural persons'

(GDPR). In practice, this includes all data that can be assigned to a person in any way, such as telephone numbers, credit card or personnel numbers, account data, license plates, appearance, customer numbers, or addresses, all of which constitute personal data (GDPR). As citizens, clients, and consumers, individuals require the means and resources to exercise their right to privacy and safeguard themselves and their data against exploitation (Privacy International). Data protection refers to laws that safeguard personal information. The term 'data protection' refers to the protection of information on an identified natural person. For AI systems to work well, a lot of personal data is frequently needed. This kind of invasive data collection may contain private communication, browsing patterns, and location data, among other sensitive data. Such data can be gathered and analysed to create comprehensive profiles that may be abused. Hackers may choose to target AI systems in an attempt to obtain personal data by taking advantage of security vulnerabilities. Such breaches may lead to financial loss, identity theft, and other types of personal injury. For example, the European Data Protection Supervisor argued that the large-scale collection of data for web advertisements exploits individuals as interchangeable data points that serve only to drive revenues (Aizenberg and Hoven). AI can discriminate, propagate prejudices, and worsen inequities, making it a major ethical concern, as algorithms are trained on previously collected data and may end up replicating undesirable patterns of unfairness from the data they process. In AI, adherence to the right to be informed may conflict with or hinder compliance with other data protection standards (Zornetta and Cofone). For example, data minimisation may need modifying training data and removing any contact information. In this situation, informing the concerned data subjects may be challenging, if not impossible (Zornetta and Cofone). AI is also susceptible to data breach too, according to Article 4(12) of the GDPR: 'personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' (GDPR). Data breach might occur through unsecured data management by AI system. Data breaches that may

substantially jeopardise data subjects' fundamental rights and freedoms (Convention 108+). Flawed data aggregation is also another concern of AI technology. Although the initial training data is representative, bias is added later in the process. It can occur in a way that AI training involves manual data aggregation, where inconsistencies in labelling can lead to automated decisions and continue to affect AI behaviour (Tischbirek). For example, If, in consumer credit decisions, the label 'creditworthy' was denied to people of colour who fell behind on three credit card repayments, while other (mostly white) individuals could fall behind on four repayments without being labelled as 'defaulting,' AI is likely to treat future cases of 'creditworthiness' similarly (Tischbirek). Another example is that AI generated recruitment tool is intended to streamline the recruiting process by filtering resumes for the best applicants; but, due to historical biases in the training datasets, it exhibits a preference for individuals from specific locations, states, and universities while penalising those with unconventional career choices (Tischbirek). As a result, talented individuals may be routinely ignored, impeding the organization's capacity to build a diverse staff and propagating prejudices. Candidates may experience unintended discrimination based on gender, colour, or education, which can have social and economic ramifications (Tischbirek). Ethnic minorities may face fewer job interview invitations due to algorithms trained on data showing worse outcomes for their group. This can be occurred when protected characteristics like gender, ethnicity, or religion are included, as well as proxy information like height or postcode. Assessing these unequal outcomes and differential treatment is crucial to preventing discrimination (European Union Agency for Fundamental Rights). An AI-powered healthcare platform uses sensitive personal data for personalised genetic analysis and medical recommendations. Breaching this data could lead to identity theft, health-related scams, insurance changes, employment issues, and reputational damage. (Tischbirek). Moreover, data protection is very sensitive and cautious, while the use of AI technology is vulnerable to its misuse.

Protection of Individual Privacy and Freedom

When creating and adopting AI applications that may have impacts on individuals and society, it is critical to respect human dignity as well as human rights and fundamental freedoms, particularly the right to the protection of personal data (European Parliament & Council of the European Union). The significant components of the approach emphasise lawfulness, fairness, purpose specification, proportionality, privacy-by-design, accountability, transparency, data security, and risk management (European Parliament & Council of the European Union). In December 2013, resolution 68/167 on the right to privacy in the digital age was adopted by the UN General Assembly without a vote. It also emphasised the necessity for States to guarantee the full and effective execution of their responsibilities under international human rights law, calling on all States to review their policies, procedures, and laws about communications monitoring, interception, and the gathering of personal data (*The Right to Privacy in the Digital Age*). Regarding nations' responsibility, government regulations should prioritise enhancing openness, guaranteeing public supervision, and safeguarding human rights. The government should also conduct surveillance that must adhere to International Principles on the Application of Human Rights to Communications Surveillance, which was produced by a coalition of civil society groups, industry leaders, and researchers (Funk et al.). Apart from governments, civil society should also be involved from the outset to establish responsible AI governance. Non-profits, journalists, and activists who have previously advocated for internet freedom can use public pressure to persuade politicians, regulators, and the industry to bring a fair AI mechanism (Funk et al.). Companies should develop effective ways to designate AI-generated information, such as using a cryptographic signature, collaborating with civil society to standardise how the industry records the origin of specific material, and investing in developing technologies that can recognise AI-generated content (Allie et al.). The principles of legal, necessary, and proportionate communications surveillance should apply to AI and biometric technologies, targeted surveillance tools like commercial spyware and extraction software,

and open-source intelligence methods like social media monitoring (Funk et al.). The companies should place limitations on the collection of personal information such as biometrics and health location data and restrict how third parties may access and use it. Companies should also fully disclose to their service users what data is being gathered and for what purpose, including what information may be obtained through user prompts to generative AI. Similarly, companies should guarantee that users have control over their data, including the ability to view, delete, and prevent it from influencing an algorithm's behaviour (Funk et al.). In many ways, the encroachment of AI on individuals' privacy and freedom can be regulated.

Conclusion

In assessing the implications of AI for freedom and privacy, it is clear that while AI holds immense potential for advancing human capabilities and improving societal outcomes, it also presents significant challenges. Business visionary Elon Musk has warned that artificial intelligence could become humanity's 'greatest existential risk', while, in contrast, futurist Ray Kurzweil offers a more optimistic view, suggesting that AI can help us make 'significant progress in addressing the world's grand challenges' (Chakraborty and Bhojwani). Around 2080, the world will be governed by AI, which will tend to integrate live people and intellect, and require humanity to defend the survival of the physical body to escape its disintegration into the virtual world (Cataleta). On a global level, individual privacy has also been safeguarded by various international conventions. Article 17 (paragraph 2) of the International Covenant on Civil and Political Rights specifically declares that everyone has the right to be protected by the law against unlawful or arbitrary interference with their privacy. This implies that any program involving the monitoring of communications must operate under a legally accessible framework that complies with both international human rights legislation and the state's own constitution (*The Right to Privacy in the Digital Age*). The intrusion of technological monitoring into individual affairs has not been widely addressed globally by many countries because they do not

have much experience with its impacts. Hence, there is some lack of effective initiatives regarding the management of AI technology. Until now, only technologically advanced countries have taken effective measures to control the AI system against its harmful impact on humans. Each day, distinct new AI technologies are coming out in various areas. Hence, there are various challenges to regulate AI. The following are the significant challenges of those (OVIC):

- AI technology is not limited to certain states or jurisdictions, making it challenging to establish and uphold effective privacy standards and governance across borders.
- Regulators face a difficult task in determining who owns, stores, and is responsible for the data.
- Good governance requires an awareness of technology. As AI develops at a rapid pace, the long-standing divide between law and technology widens, as does the complexity and scope of AI's applications.
- The extent to which the government should regulate AI emphasises that the lack of a legal framework for AI in terms of information privacy is a regulatory decision in and of itself.

However, if we need to overcome such regulatory challenges, some ideational and practical measurements have to be adopted. Firstly, transparency should be there in making sure decisions made by AI can be explained and comprehended. Secondly, accountability should be there for keeping organisations accountable for the impact of their AI systems. Thirdly, fairness should be kept by freeing AI systems from discrimination and bias. Fourthly, security and privacy protection mechanisms should be enhanced to safeguard data and protect AI system security. Fifthly, there should be human oversight when crucial decisions are made by the AI systems. It is also essential to instil ethical norms in AI because, as it becomes more autonomous, it will increasingly pose and need to address moral dilemmas; however, when establishing these norms, prioritizing human rights must be a fundamental concern (Cataleta). The future of AI is dependent on our shared commitment to developing systems that respect and defend the principles of human dignity and privacy.

Key Recommendations

Regulatory and Legal Frameworks: There is a need to adopt comprehensive legislation, especially in the area of robust data protection laws. At the same time, there is a need for regulatory oversight to regulate the use of AI and ensure compliance with privacy and freedom requirements. For examples, the European Union's General Data Protection Regulation (GDPR) (to protect the privacy and security of individuals), GPAI (Global Partnership on AI) (global initiative, involving the US, UK, Canada, and France, promotes ethical and human-centered research and application of artificial intelligence), Algorithmic Accountability Act of United States (The proposed legislation requires companies to conduct impact assessments on automated decision systems to evaluate their effectiveness and potential biases), China's new AI regulations (the Chinese government's guidelines on ethical AI use focus on security, fairness, and transparency to promote innovation and control its societal impacts). India's National Strategy for Artificial Intelligence (it is an approach emphasises inclusivity, accountability, and openness while utilising AI to promote social and economic progress). Laws have also been initiated to restrict private firms from using personal data for AI research, algorithms, and recommendations.

Transparency and Accountability: Individuals should have control over their data, including the right to view, delete, and transfer it to preferred providers. Designing AI systems that provide clear, intelligible explanations for their judgements, thereby increasing openness and accountability. For example, if a bank instils an AI-powered loan approval mechanism, it can assess several factors, including credit ratings, employment history, income, and spending habits, before approving or denying loans. There is a need to conduct regular audits and impact evaluations to assess the ethical implications and privacy risks.

Enhanced Technologies for Privacy: Data minimization strategies need to adopt techniques that limit the amount of data collected to what is required for the intended purpose, lowering the risk of misuse. Strong encryption is necessary to safeguard data in transit and at rest, ensuring that unauthorised parties do not have access to sensitive information. The individuals should be informed about the data that

is collected, used, and shared and obtain explicit consent for data processing activities. Individuals should be allowed to quickly access and transfer their data between multiple service providers, thereby increasing their control over personal information.

Fair AI Practice: The strategies that are applied have to detect and mitigate biases in AI systems. And it should be ensured that there is no perpetuated discrimination or unfair treatment. Inclusive data management is needed because using broad and representative datasets to train AI systems reduces the possibility of biased results.

Digital Literacy: The purpose of digital literacy is to encourage and inform people about their rights and the possible effects of artificial intelligence on freedom and privacy. It is also promoting public discussion and activism on the moral application of AI, as well as cultivating an environment of accountability and responsibility among users and developers.

References

- Abhivardhan. "The Privacy Doctrine." *Artificial Intelligence Ethics and International Law Practical Approaches to AI Governance*, BPB Online, 2024.
- Aizenberg, E., and Jeroen van den Hoven. "Designing for Human Rights in AI." *Big Data and Society*, vol. 7, no. 2, 2020.
- AUDA-NEPAD. *AI for Africa: Artificial Intelligence for Africa's Socio-Economic Development*. African Union Development Agency, 2021.
- Cataleta, Maria Stefania. "Humane Artificial Intelligence: The Fragility of Human Rights Facing AI." *East West Center Working Paper No. 2*, 2021.
- Chakraborty, Swatilekha, and Rishabh Bhojwani. "Artificial Intelligence and Human Rights: Are they Convergent or Parallel to Each Other?." *Novum Jus*, vol. 12, no. 2, 2018, pp. 14-42.
- Chirag. "How AI is Transforming Traditional Surveillance Systems." *Appinventiv*. 2024.
- Convention 108+. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. 2018.
- European Parliament & Council of the European Union. *EU General Data Protection Regulation*. 2016.
- European Union Agency for Fundamental Rights. *#BigData: Discrimination in Data-Supported Decision Making*. 2018.
- European Union Agency for Fundamental Rights. *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*. 2019.
- Feldstein, Steven. *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace, 2019.
- Funk, Allie, et al. "Freedom on the Net 2023: The Repressive Power of Artificial Intelligence." *Freedom House*, 2023.
- Golunova, Valentina. "Artificial Intelligence and the Right to Liberty and Security." *Artificial Intelligence and Human Rights*, edited by Alberrio Quintavalla and Jeroen Temperman, Oxford University Press, 2023, pp. 45-60.
- González, Natalia Menendez. "The Rights to Privacy and Data Protection and Facial Recognition Technology in the Global North." *Artificial Intelligence and Human Rights*, edited by Alberrio Quintavalla and Jeroen Temperman, Oxford University Press, 2023, pp. 136-49.
- Lee, Jootaek. "Artificial Intelligence and Human Rights: Four Realms of Discussion: Summary of Remarks." *Proceedings of the ASIL Annual Meeting*, vol. 114, 2020, pp. 242-45.
- MeitY. *On Cyber Security, Safety, Legal and Ethical Issues*. Ministry of Electronics & Information Technology, Government of India, 2022.
- Mozur, Paul. "One Month, 500,000 Face Scans: How China is using AI to Profile a Minority." *The New York Times*, 2019.
- NITI Aayog. *National Strategy for Artificial Intelligence*. 2018.
- OVIC. "Artificial Intelligence and Privacy – Issues and Challenges." *Office of the Victorian Information Commissioner*. 2018.
- Privacy International. *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection*. 2018.
- Stahl, Bernard Carsten, et al. "A European Agency for Artificial Intelligence: Protecting

- Fundamental Rights and Ethical Values." *Computer Law & Security Review*, 2022.
- Stanford University. *Artificial Intelligence and Life in 2030*. 2016.
- The Economic Times. "AI and Privacy: The Privacy Concerns Surrounding AI, Its Potential Impact on Personal Data." *The Economic Times*, 2023.
- The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*. United Nations Digital Library, 2014.
- Tischbirek, Alexander. "Artificial Intelligence and Discrimination: Discriminating against Discriminatory Systems." *Regulating Artificial Intelligence*, edited by Thomas Wischmeyer and Timo Rademacher, Springer, 2020.
- United Nations. "Universal Declaration of Human Rights." *United Nations*.
- United Nations. *International Covenant on Civil and Political Rights*. 1966.
- Warzel, Charlie. "A Major Police Body Cam Company Just Banned Facial Recognition." *The New York Times*, 2019.
- WHO. *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance*. World Health Organization, 2021.
- WSU. "Challenges of AI." *Washington State University*.
- Zornetta, Alessia, and Ignacio Cofone. "Artificial Intelligence and the Right to Privacy." *Artificial Intelligence and Human Rights*, edited by A. Quintavalla and Jeroen Temperman, Oxford University Press, 2023.

Author Details

Dr. Binu Joseph, Assistant Professor, NA Global Law School, Bangalore, Karnataka, India,

Email ID: binuj5555@gmail.com