



Artificial Intelligence (AI) Technology: Negative Impacts on Fundamental Rights Protected by International Human Rights Law*

Stanati Netipatalachoochote**

Maythavee Buasomboon***

■ Abstract

Artificial Intelligence (AI) has become increasingly embedded in everyday life across diverse domains, including chatbots, credit scoring, image and video generation and graphic design, AI robotic surgery, and more. Although AI is considered as a technology that improves human efficiency and convenience in many aspects, the negative impacts that may arise from its use can also lead to various problems. Therefore, the purposes of this research are to (1) examine how AI can produce negative effects by its operation, leading to the erosion of data protection and privacy, generating bias and discrimination, and reducing transparency in operational mechanisms; and (2) demonstrate how the use of AI technology can lead to violations of five international human rights laws that guarantee fundamental rights; The analysis draws on materials collected during 2024 through the end of February 2025. The findings indicate that the

* This article is a research project funded by Siam University, Bangkok, Thailand, and the NSRF via the Program Management Unit for Human Resources & Institutional Development, Research and Innovation (PMU-B) [grant number BI3F670126].

** Lecturer, International College & Global Academy, Siam University

*** Lecturer, the Faculty of Law, Siam University

Received: 6 February 2025 Revised: 11 December 2025 Accepted: 22 January 2026

use of AI can adversely affect fundamental rights in multiple everyday contexts. The study categorizes these impacts into six areas: (1) online service platforms usage; (2) transportation and logistics; (3) financial services; (4) education and human resources; (5) healthcare; and (6) law enforcement by state officials. The study also highlights recent policy and legal developments in the European Union, particularly the EU AI Act (2024), as a rights-oriented regulatory framework that sets baseline conditions and requirements intended to mitigate negative effects on fundamental rights arising from AI deployment.

Keywords: Artificial Intelligence (AI) Technology, Negative Impacts, Fundamental Rights, Policy and Law

■ Introduction

Artificial Intelligence (AI) is one of the innovations that has transformed the daily lives of humans, making various activities more convenient, timely, and efficient. Beyond simply unlocking a mobile phone to daily activities such as online shopping, self-driving cars, and robots for customer convenience, artificial intelligence is also a driving factor behind advancements in

the economy, medicine, and government operations. The key principle of AI function is the assessment of vast amounts of data and delivering it in a way that meets human needs as efficiently and quickly as possible. AI applications are used for a variety of purposes, especially in human daily life. Examples of well-known AI applications as of the year 2024 is illustrated in Table 1 below

While AI has contributed to significant advancements for humanity, it also poses numerous risks and negative impacts, particularly on fundamental rights as enshrined in various international human rights laws and treaties signed and ratified by numerous countries (Rodrigues, 2020). The potential impacts of AI on fundamental rights arise from several factors (European Union Agency for Fundamental Rights: FRA, 2020), such as insufficient transparency of algorithms, cybersecurity vulnerabilities, issues of bias, unfairness, and discrimination, lack of mechanisms for contesting AI decisions, concerns over legal personhood and ethical responsibility, privacy and data protection issues, liability issues related to damages caused by AI, and inadequate accountability for harms.

Nevertheless, this research focuses on identifying the negative impacts of AI by addressing concrete issues rooted in

Table 1 An Example of Well-Known AI Applications Tried and Used in 2024

Purposes / Functions	AI symbols
Chatbots, Writing, Grammar Checking	 ChatGPT  wordtune  Claude  Rytr  grammarly  SUDOWRITE
Image and Video Generation and Graphic Design	 runway  synthesia  Canva  Looka
Customer Service, Work Scheduling	 TIDIO  hiver  reclaimai  clockwise  agendrix
Resume Builders, Recruitment and Human Resources	 Textio  CVViz  kickresume  Rezi  resume.io
Healthcare, and Medical Services	 Insilico Medicine  ada  prognos health

Note: From "What Are the Most Used Generative AI Tools in 2024?", by Isarta. 2024, Isarta. <https://isarta.com/news/what-are-the-most-used-generative-ai-tools-in-2024/>

the daily lives of individuals, rather than abstract concepts or internal components of AI systems, which is different from those above described by FRA and Rodrigues. The study adopts an approach that analyzes the negative effects of AI specifically within

activities that are directly connected to human daily life. The evaluation framework includes the following topics: (1) Online Service Platform Usage; (2) Transportation and Logistics; (3) Financial Services; (4) Education and Human Resources;

(5) Healthcare; (6) Law Enforcement by State Officials.

Research Objectives

(1) To highlight that the use of AI leads to negative impacts stemming from the operational methods of AI itself, resulting in the erosion of data boundaries and human privacy, creating bias and discrimination, and a lack of transparency in operational mechanisms.

(2) To demonstrate how the use of AI results in violations of five international human rights laws that guarantee fundamental rights.

(3) To propose that the EU AI Act, as the first regulatory framework in the world, where fundamental rights are one of the purpose of this law, shows some aspect, and criteria to prevent the adverse impact on fundamental rights might be caused by AI technology.

Research Methodology

This legal research is conducted through a qualitative method by exploring laws, policies, documents, and case studies. An analysis is performed here by using the database collected by the end of 2024. The research is facilitated by access to resources at the Centre for Research in Private International Law, Faculty of Law, University of Lyon III, France,

allowing the researcher to conduct research from March 2024 to April 2025, particularly focusing on international databases and those related to the European Union. Additionally, it includes synthesizing information from personal interviews—the expert from the European Union Agency for Fundamental Rights, group discussions—academic work on an AI approach, based in French universities, from different sections such as legal, medical, economic, and political science fields. Also, the analysis of the raw data in conjunction with the documentary information was conducted.

Particularly, this study employs indicators of violations of fundamental human rights, using international human rights laws as a standard to determine which provisions the use of AI can potentially violate. The analysis focuses on five key international and regional human rights treaties: (1) The Universal Declaration of Human Rights (UDHR), 1948; (2) The International Covenant on Economic, Social and Cultural Rights (ICESCR), 1966; (3) The International Covenant on Civil and Political Rights (ICCPR), 1966; (4) The Charter of Fundamental Rights of the European Union (CFR), 2000; and (5) The European Convention on Human Rights (ECHR), 1950, also known as the Convention for the Protection of Human Rights and Fundamental Freedoms.

Literature Review and Theoretical Framework:

1. The evolution of artificial intelligence technology and its current applications.

In 1950, Alan Mathison Turing, a British scientist, initiated the exploration of the mathematical potential of AI. He developed the "Turing Test," a practical evaluation aimed at assessing the intelligence of computers, based on the idea that machines should be able to utilize available data to solve problems and make decisions like humans (Black, 2023, pp. 442-464). Later, during the summer of 1956 at the Dartmouth College Conference, significant advancements were made in creating a "Thinking Machine" by Allen Newell, a researcher in computer science and cognitive psychology, and Herbert Alexander Simon, an economist and psychologist. The program developed by these two experts was a computer program capable of proving theorems in symbolic logic, which later appeared in the book "Principia Mathematica" (Cordeschi, 2007, pp. 259-279; Gugerty, 2006, pp. 880-884).

The evolution of AI has continued to progress, marked by the emergence of "Deep Learning" in the 1990s. This advancement represented a significant milestone in the field of AI and attracted considerable attention from researchers across various disciplines during that

era (LeCun et al., 2015, pp. 436-444). Subsequently, since the mid-2000s, the world has witnessed a major transformation driven by Big Data and the development of computational tools, such as Graphics Processing Units (GPUs) and the Rectified Linear Unit (ReLU) function. These innovations have been increasingly utilized in Machine Learning processes, leading to widespread adoption and further advancements in the field.

In 2012, the field of AI reached a new level of development with the introduction of a neural network called AlexNet, developed by Alex Krizhevsky, Ilya Sutskever, and Geoffrey Hinton. This neural network was employed in the ImageNet competition, a computer science competition focused on object classification in images sourced from the internet, spanning 1,000 possible categories. The ImageNet competition serves as a benchmark for evaluating the performance of deep learning models, particularly convolutional neural networks (CNNs) (Krizhevsky et al., 2017, pp. 84-90). AlexNet not only won the competition but also outperformed competitors by an unprecedented margin. This success provided compelling evidence of the significant advancements that Deep Learning technology has brought to the field of AI.

The advancements in AI expanded into the gaming industry between 2016 and 2019 with the introduction of MuZero, a system demonstrating superhuman capabilities in playing games such as Go, chess, and shogi (Japanese chess). MuZero represents an advanced algorithm leveraging AI to plan winning strategies in unfamiliar environments, enabling it to succeed without prior knowledge of the rules of the respective games. Furthermore, the AlphaGo system, which incorporates MuZero's algorithm, made headlines by defeating Lee Sedol, an 18-time world champion and Go expert (Schrittwieser et al., 2019). The emergence of Generative Language AI after 2020 highlighted the rapid evolution of AI. This type of AI, exemplified by applications such as PaLM and Minerva, showcased its ability to produce high-quality text comparable to human writing, explain jokes, clarify cause-and-effect relationships, and solve complex university-level mathematics problems (Roser, 2022).

Today, global society is driven by digital systems powered by AI, which plays a critical role in enabling societies to adapt and navigate through rapid changes. AI has had a significant impact on the global economy and key industries such as engineering, agriculture, politics, mass media, medicine, and education. This technology has also

enhanced systems for delivering, creating, disseminating, and storing information with efficiency, precision, and, in some cases, greater stability than human efforts (Gil et al., 2024, pp. 317-334). The advancements in AI demonstrate its capabilities across various fields, including computer vision, machine translation, medical diagnosis, voice recognition, and the autonomous creation of text, images, and video content (Jungherr, 2023).

These AI technologies have also enabled machines to integrate more seamlessly into human daily activities and play a pivotal role in decision-making processes traditionally carried out by humans. Examples include loan approvals, assessments for welfare eligibility, recruitment processes, AI-assisted robotic surgery, and decisions on releasing inmates from correctional facilities. In addition to these applications, AI plays a key role in developing software and tools used in everyday life, such as AI translation tools and virtual assistants capable of generating sentences, contexts, and written content. These technologies have become commonplace in global society. For instance, "Generative AI" tools like ChatGPT, launched in late 2022, have created transformative impacts on both social and economic landscapes. However, alongside these advancements, significant concerns have arisen. These include the potential

replacement of human labor in certain professions and the proliferation of misinformation, which could have far-reaching consequences on the freedoms and rights of AI users (Carvalho & Ivanov, 2024, pp. 290-303; Curtis, 2023, p. 275).

The continuous development of AI has brought about a variety of challenges related to legal and fundamental rights issues. For instance, in the case of AI-driven autonomous vehicles, if such a vehicle causes an accident, such as hitting a pedestrian, complex legal liability issues arise. These include determining responsibility between the manufacturer and the vehicle owner, particularly addressing questions such as whether the manufacturer's liability ends completely upon selling the vehicle to the buyer. If there are arguments that the AI system lacks sufficient stability or safety, should the manufacturer share liability or bear separate responsibility from the vehicle owner? Furthermore, how should liability be determined in such scenarios? If the AI system is argued to be unstable or insufficiently safe, it may open the door for the manufacturer to share or separately bear responsibility apart from the vehicle owner. Other important issues include establishing rules and regulations for obtaining driving licenses for AI-operated vehicles and determining the technological knowledge required to support laws

that regulate or permit the operation of such vehicles. These challenges demand practical solutions (Kubica, 2022, pp. i39-i69). From this case, the necessity for new laws or amendments to existing legislation to address these issues and provide remedies for affected parties is therefore warranted. This process must carefully incorporate considerations of fundamental rights. Developing clear and precise legal measures is essential for effectively protecting victims affected by AI-driven devices and the damages they may cause (Harrison, 2023).

Research Findings and Discussion:

1. Negative Impacts caused by AI on Fundamental Rights, analysed under Five International Human Rights Law Instruments.

1.1 Online Service Platforms Usage

The pandemic marked a period of significant global transformation, ushering in a new era of technology integration across various sectors. One of the most notable changes has been the sharp rise in the use of online shopping services, accompanied by increasingly intense competition within the industry. AI has become a critical component for online businesses. According to statistics, the use of AI in online commerce was valued at \$8.65 billion in 2025, with projections

estimating it to reach \$17.1 billion by 2030 (Jason, 2024). While AI offers significant advantages, such as improved customer service, personalized recommendations, and efficient inventory management, its integration into online platforms raises concerns about fundamental rights. These concerns include data privacy, consumer discrimination through algorithmic profiling, and the potential for monopolistic practices fueled by advanced predictive analytics. As the reliance on AI grows, addressing these impacts becomes essential to safeguard users' rights in the digital marketplace.

AI can be applied to various aspects of online commerce, including sales prospecting and forecasting. AI enables e-commerce platforms to identify and evaluate customer profiles, allowing them to define target groups with greater precision and speed. It can tailor messages, recommendations, and content to align with individual preferences and behaviors, assess sales calls, provide sellers with strategic advice, and deliver valuable insights into customer behavior and preferences. This capability significantly enhances customer engagement and satisfaction, though it also raises concerns about overreliance on automation. AI facilitates precise marketing by enabling sellers to target audiences effectively and

attract purchases through promotions or campaigns designed specifically for these groups, outperforming traditional marketing methods.

Additionally, AI employs sales automation techniques, such as automated follow-up emails and updates in Customer Relationship Management (CRM) systems, to streamline the sales process. These innovations provide businesses with a more efficient way to manage customer relationships and improve operational productivity (Mittal et al., 2024, pp. 159-173). While these advancements offer significant benefits to businesses and consumers, they also pose potential risks, including reduced transparency in automated decision-making, customer manipulation through algorithmic targeting, and privacy concerns arising from extensive data collection and analysis. These issues highlight the need for balanced AI integration in online commerce to protect fundamental rights.

The capabilities of AI mentioned earlier can have negative impacts on users, particularly online shoppers or service users, especially regarding fundamental rights enshrined in international human rights laws. Specifically, consumer protection rights, as outlined in Article 38 of the Charter of Fundamental Rights of the European Union (CFR), emphasize that

consumer rights must be safeguarded during service provision. AI has the potential to infringe upon these rights through its role in service delivery, as discussed, and through additional functionalities such as tailored shopping suggestions, virtual shopping assistants, fabricated product reviews, and chatbots for customer support and recommendations. These features may negatively affect consumers by enabling unfair, biased, or erroneous decision-making.

Moreover, AI can influence consumer decisions in ways they did not initially intend. For instance, AI tools may analyze historical consumer data to make recommendations, subtly steering consumers toward decisions they may not consciously recognize. This can result in consumers purchasing or using services they no longer desire or need, based solely on patterns of past behavior. Such manipulation complicates consumers' ability to discern whether their choices are genuinely autonomous or are being influenced by AI-driven algorithms. These concerns highlight the importance of monitoring and regulating AI in e-commerce to ensure transparency, fairness, and the protection of consumer rights, as prescribed by international human rights standards.

In the context of content creation by sellers using AI for marketing purposes, AI can have negative impacts

on vulnerable groups such as children, individuals with impaired maturity, the elderly, or those with mental health conditions. Exposure to or access to AI-generated content, messages, images, or sounds used for marketing purposes could constitute a violation of the rights of the child, as outlined in Article 24 of the International Covenant on Civil and Political Rights (ICCPR) and Article 24 of the Charter of Fundamental Rights of the European Union (CFR). AI-generated content may inadvertently produce harmful material for children, such as rude language, sexually explicit or pornographic images, or content that incites illegal or inappropriate behavior. Such content could be created and disseminated without ethical considerations, as AI systems often lack the ability to exercise moral judgment, self-monitor, or carefully review their outputs prior to publication. Additionally, certain types of AI-generated content might reflect or perpetuate gender inequality, which is protected against under Article 3 of the International Covenant on Economic, Social and Cultural Rights (ICESCR) and Article 23 of the Charter of Fundamental Rights of the European Union (CFR). These issues underscore the importance of implementing ethical guidelines and robust oversight mechanisms to prevent AI-generated content from causing harm or violating fundamental

rights, particularly for vulnerable groups such as children.

1.2 Transportation and Logistics

The advent of AI, particularly in the form of automation, has brought significant transformations to the transportation and logistics industry. AI has improved efficiency, accuracy, and speed in logistics operations, while also enhancing the infrastructure of logistics systems (Pshychenko, 2024, pp. 64-67). One notable application is inventory management, where AI algorithms are used to forecast demand and optimize inventory levels, thereby reducing the risks of overstocking or stockouts. This improvement leads to better accuracy in inventory management and reduced holding costs. A prime example is Amazon, which employs AI-driven predictive analytics to streamline its inventory management. Another key area is transportation optimization. AI enables the analysis of traffic patterns, weather conditions, and other factors to plan optimal transportation routes. This not only reduces transportation costs but also improves delivery times and lowers carbon emissions. Another example is UPS, which uses its AI-powered ORION system to optimize package delivery routes, demonstrating significant gains in efficiency and sustainability. These advancements underline the potential of AI to revolutionize

logistics and transportation. However, as these technologies continue to develop, it is essential to consider their potential legal and ethical implications, particularly in the context of labour displacement, data privacy, and environmental impact.

AI further contributes to predictive maintenance in logistics systems by monitoring equipment conditions and predicting potential issues before they result in damage. This approach helps reduce maintenance costs and extends the lifespan of equipment, ensuring smoother operations. Lastly, AI enhances supply chain visibility, enabling better tracking and management of global logistics operations. For instance, Maersk leverages AI to monitor and manage its worldwide shipping activities, fostering transparency and efficiency throughout the supply chain. These applications highlight AI's transformative impact on logistics and transportation, driving efficiency, sustainability, and enhanced customer satisfaction. However, it also raises important considerations regarding data privacy, ethical practices, and the need for appropriate regulatory frameworks.

However, despite the convenience AI brings to logistics systems, its negative impacts must also be considered, particularly those affecting fundamental human rights. Firstly, if AI systems fail

in logistics processes—such as delivery delays or failure to provide satisfactory service—customers may find it difficult to access justice, a right protected under Article 8 of the Universal Declaration of Human Rights (UDHR), Article 14 of the International Covenant on Civil and Political Rights (ICCPR), and Article 6 of the European Convention on Human Rights (ECHR). For example, if AI-driven chatbots are used in dispute resolution, their responses might lack clarity or even distort facts, potentially favoring companies over consumers. This could allow businesses employing AI to evade accountability, undermining the consumer's ability to seek fair legal recourse. Such issues directly affect the right to effective remedy, as guaranteed by Article 13 of the ECHR and Article 47 of the Charter of Fundamental Rights of the European Union (CFR). If AI systems, such as chatbots, are programmed to prioritize the company's interests, consumers may struggle to obtain fair outcomes or effective remedies, further eroding their fundamental rights.

Another notable impact on fundamental human rights is the collection and storage of customer data and delivery details by AI systems in logistics. Ensuring the privacy and security of this data is crucial to prevent cyber theft, data breaches,

and unauthorized access, as these issues constitute violations of data protection rights outlined in Article 8 of the Charter of Fundamental Rights of the European Union (CFR) and the right to privacy free from interference stated in Article 12 of the Universal Declaration of Human Rights (UDHR). Recognizing the importance of protecting personal data, many countries worldwide have enacted specific laws to prevent and address data breaches. Notably, the European Union's General Data Protection Regulation (GDPR) (The Regulation (EU) 2016/679) serves as a comprehensive framework for data protection and privacy. Similarly, Thailand has implemented the Personal Data Protection Act, B.E. 2562 (2019) to safeguard personal data from unauthorized use and breaches. These legal frameworks emphasize the necessity of establishing clear and enforceable measures to ensure that AI systems in logistics uphold data protection standards, thereby preserving individuals' fundamental rights to privacy and security in an increasingly digitized world. These concerns highlight the need for robust legal frameworks and oversight to ensure AI applications in logistics are transparent, fair, and respectful of basic human rights, particularly in contexts where justice and remedy are at stake.

1.3 Financial Services

AI has been widely adopted to enhance the convenience and efficiency of financial services in various dimensions. AI serves as an automated financial advisor, helping users manage and make decisions regarding financial challenges they face. It tracks users' financial goals, analyzes stock market trends, and provides recommendations on which stocks or bonds to buy or sell (Chakraborty & Joseph, 2017). AI wallets also play a significant role by studying users' spending patterns and preferences and offering suggestions to promote better spending discipline. These tools are often provided by banks to facilitate better financial management for their customers. Customers can leverage these AI-driven tools to perform transactions and access information quickly, particularly for routine inquiries that AI systems are programmed to respond to automatically. This enhances customer convenience by providing real-time assistance and improving service efficiency (Srinadi et al., 2023, pp. 106-117). While these innovations offer significant benefits, they also pose challenges, including concerns about data privacy, algorithmic biases in financial recommendations, and the potential for misuse of customer data. These issues highlight the importance of ethical and transparent AI use in financial services

to ensure trust and the protection of consumer rights.

Banks have enhanced their capabilities by utilizing AI to collect data and monitor customer spending behaviours. This enables them to provide more reliable and tailored financial advice and services to their customers. AI allows banks to track the financial status and growth of their customers' businesses, which can then be analyzed to assess their financial standing for various transactions or services, such as loans, mortgage approvals, insurance purchases, credit card approvals, and fund investments (Kaur et al., 2020). By leveraging these AI-driven insights, banks can offer more personalized services, streamline decision-making processes, and improve overall customer satisfaction. However, such extensive data collection and analysis also raise concerns regarding data privacy and the ethical use of customer information, highlighting the need for robust regulatory measures to ensure the responsible use of AI in financial services.

One of the significant issues arising from the use of AI in financial services, particularly concerning fundamental rights, is the rejection of loan applications by banks or financial institutions. Decisions that were previously made by human officials responsible for approving such requests are now increasingly delegated

to AI systems under the assumption that AI provides greater accuracy and can analyze large datasets more effectively than humans. AI-driven decisions are often based on risk assessments derived from large datasets, including behavioral data collected from loan applicants (Adwan & Aladwan, 2022, pp. 1223-1232). However, this can result in loan rejections based on outdated, irrelevant, or inaccurate information that may not truly reflect the applicant's financial situation. Such decisions can lead to discrimination, violating Article 2 of the Universal Declaration of Human Rights (UDHR), Article 21 of the Charter of Fundamental Rights of the European Union (CFR), and Article 14 of the European Convention on Human Rights (ECHR).

Moreover, AI-driven loan rejections may unjustly impact an individual's standard of living. Those denied loans might find themselves unable to sustain their livelihoods or pursue opportunities for economic stability and growth. This violates the right to an adequate standard of living as stipulated in Article 11 of the International Covenant on Economic, Social and Cultural Rights (ICESCR). Additionally, the personal data of loan applicants, often a key component in AI risk assessments, is vulnerable to breaches or unauthorized access. This constitutes a violation of the

right to privacy, as protected under Article 8 of the Charter of Fundamental Rights of the European Union (CFR), and Article 12 of the Universal Declaration of Human Rights (UDHR). These challenges underscore the importance of balancing technological advancements with the protection of fundamental rights. Regulatory oversight, transparency in AI decision-making, and mechanisms for accountability are critical to ensuring fair and just financial services for all.

1.4 Education and Human Resources

AI is profoundly revolutionizing modern education. AI algorithms and applications have become essential components of learning management systems, training programs, and support for teaching and learning activities in various formats (Costa et al., 2017, pp. 247-256). Numerous AI-powered applications have been developed to enhance educational experiences. For example, Khanmigo assists in various subjects, including mathematics, programming, and language learning, while platforms like Duolingo leverage AI to enrich language learning experiences. Additionally, iFlyTek, an AI system for intelligent assessment, adapts to diverse scoring scenarios, including university entrance exams (Wang et al., 2024). These AI tools significantly improve personalized learning, providing students with tailored

feedback and enabling educators to efficiently evaluate and adapt teaching strategies. By enhancing accessibility and efficiency in education, AI contributes to reshaping traditional learning environments, preparing students for future challenges in an increasingly digital world. However, the integration of AI in education also raises concerns about data privacy, equity in access to AI tools, and the ethical implications of relying on algorithm-driven assessments. Addressing these challenges is crucial to ensure that AI in education upholds fundamental rights and promotes inclusive and fair learning opportunities.

AI poses significant risks and challenges to fundamental rights in education, particularly in areas such as automated admissions systems and performance assessments. University admissions processes often involve grading, portfolio reviews, and application assessments, requiring the collection and analysis of substantial personal data from applicants. If AI systems used for data management and evaluation experience errors or data breaches, this constitutes a violation of the right to privacy under Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 8 of the Charter of Fundamental Rights of the European Union (CFR). Furthermore, these systems can unintentionally perpetuate bias

and inequitable practices. Applicants from different financial backgrounds may have varying abilities in preparing applications, leading to unequal consideration. Access to AI-assisted tools for preparing applications or interviews might favour wealthier applicants who can afford advanced technologies or AI services, while those with limited resources may struggle to create compelling applications.

This disparity can result in unfair advantages for some and limited opportunities for others, even though education should be a universally accessible right. Fundamental rights potentially violated in these cases include the right to equal access to public services as stated in Article 21 of the Universal Declaration of Human Rights (UDHR), the right to an adequate standard of living as outlined in Article 25 of the UDHR, and Article 11 of the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the right to education under Article 26 of the UDHR, Article 13 of the ICESCR, and Article 14 of the CFR. These challenges underline the importance of implementing robust regulations and ethical guidelines to ensure that AI systems used in education are transparent, and fair, and do not reinforce inequalities, thereby safeguarding fundamental rights and promoting equal access to educational opportunities.

These impacts extend further into the realm of employment, where the initial stages of job recruitment often involve searching and applying for jobs. In these processes, the privacy rights of job seekers and applicants may be compromised, similar to the concerns raised in the context of educational admissions. Job seekers are required to disclose personal information to potential employers or provide it to job-matching applications, leading to their data being disseminated to an increasing number of public and private entities. AI systems are frequently utilized in recruitment processes to manage large volumes of applications efficiently, addressing the challenge of processing an overwhelming number of submissions that would be impractical for human recruiters to handle effectively.

However, this reliance on AI introduces significant responsibilities for employers and intermediary companies to securely store, manage, and protect the data involved in these processes. The use of AI in recruitment entails handling large datasets, often containing sensitive personal information. Any failure in safeguarding this data can directly infringe on the right to personal data protection as outlined in Article 8 of the Charter of Fundamental Rights of the European Union (CFR) and the right to privacy free from interference

as stated in Article 12 of the Universal Declaration of Human Rights (UDHR). These concerns underscore the critical need for stringent data protection measures and ethical frameworks in AI-driven recruitment processes to ensure that the privacy and rights of job seekers are respected and safeguarded.

In recruitment processes, the use of AI to make selection decisions may lead to unfair outcomes, similar to the concerns previously discussed in the context of education. This is primarily due to the data fed into AI systems, which may lack a transparent ethical framework for processing information and may be influenced by biases inherent in the training data. For instance, in the recruitment of university lecturers specializing in international law, AI might be used to shortlist candidates who possess a doctoral degree in the field. However, if the AI system is programmed rigidly, it may exclude candidates who, despite holding doctoral qualifications in international law, have specialized in subfields such as international human rights law or international criminal law. These candidates could possess relevant teaching experience and qualifications but might still be excluded during the initial application screening phase simply because their profiles do not match the AI's narrowly defined criteria. Such outcomes

highlight the potential for inappropriate decision-making by AI, depriving qualified individuals of the opportunity to progress to the interview stage. This issue underscores the absence of nuanced understanding and judgment in AI systems, which rely on preset parameters that may not fully reflect the complexity of human qualifications and experiences.

This concern was corroborated by an interview conducted on December 3, 2024, with the Human Resources Department of the University of Lyon III in France. The discussion revealed that the AI-based screening of applications for faculty positions in the Faculty of Law had led to such issues during the 2024 recruitment cycle. The example demonstrates the need for ethical and transparent AI frameworks in recruitment processes to ensure fairness, inclusivity, and the avoidance of biased or overly rigid decision-making criteria. It also highlights the importance of incorporating human oversight into AI-driven systems to prevent the exclusion of qualified candidates due to the limitations of algorithmic processing.

The use of AI in recruitment processes can exacerbate biases in candidate selection, particularly those related to data quality and gender. A notable example involves an AI hiring algorithm trained on data from Google News, which

exhibited bias in associating specific jobs with men and women, as well as between candidates with and without disabilities (Zhuang & Goggin, 2024). Moreover, certain screening systems have been criticized for discriminatory practices. For instance, the product HireVue, which claims to use “scientifically proven algorithms” to identify successful employees, evaluates candidates based on facial movements and vocal cues from self-recorded smartphone videos. Such methods risk violating fundamental human rights concerning non-discrimination, as outlined in Article 2 of the Universal Declaration of Human Rights (UDHR), Article 21 of the Charter of Fundamental Rights of the European Union (CFR), and Article 14 of the European Convention on Human Rights (ECHR).

These practices are particularly concerning for individuals with disabilities, such as those who are hearing or visually impaired, individuals with speech difficulties, or those who have experienced paralysis. The facial expressions or vocal characteristics of these individuals may differ from normative expectations, leading to exclusion or unfair treatment by AI systems. This constitutes a violation of the rights of persons with disabilities, as enshrined in Article 26 of the Charter of Fundamental Rights of the European

Union (CFR). Such examples highlight the critical need for ethical AI development and transparent practices in recruitment to ensure fairness and inclusivity. Establishing safeguards and implementing human oversight in AI-driven hiring processes are essential to prevent discriminatory outcomes and to uphold the fundamental rights of all individuals, particularly those from vulnerable groups.

AI also has the potential to replace human labour, such as through the use of AI-powered robots, leading to unemployment and violations of fundamental rights. These include the right to work, the right to equal pay, and the right to protection against unemployment, as guaranteed by Article 23 of the Universal Declaration of Human Rights (UDHR), Articles 6–8 of the International Covenant on Economic, Social and Cultural Rights (ICESCR), and Articles 15, 27, and 31 of the Charter of Fundamental Rights of the European Union (CFR).

Furthermore, the displacement of workers by AI can undermine the right to an adequate standard of living, which encompasses access to food, clothing, housing, and property. This right is protected under Article 25 of the UDHR, Article 11 of the ICESCR, and Article 17 of the CFR. As industries increasingly adopt AI to enhance productivity and efficiency, the

replacement of human workers by automated systems can lead to widespread job displacement, particularly in sectors that rely heavily on routine or manual labor. This situation risks deepening economic inequalities and exacerbating the struggles of individuals and families to maintain basic living standards. The ethical integration of AI in the workforce requires careful policy planning and regulatory oversight to balance technological advancements with the protection of workers' rights. Measures such as reskilling programs, unemployment protection schemes, and frameworks that promote equitable access to employment opportunities are essential to mitigate the negative impacts of AI on human labor and ensure compliance with fundamental rights.

1.5 Healthcare

AI has significantly transformed the medical field, particularly in the aftermath of the COVID-19 pandemic. Healthcare professionals, who previously relied primarily on their human skills and expertise, can now reduce the time and cost of their work with the support of AI technology. AI applications in healthcare are diverse, ranging from gene discovery tools, robotic surgery without human intervention, AI-driven medical management, customization of treatment options, and enhancement of medical diagnostics,

to health data management. AI also plays a pivotal role in advancing drug research and development. In the past, the pharmaceutical industry faced significant delays due to high development costs and the immense time required for human-led research. For instance, bringing a new drug to clinical trials used to cost an average of \$1.3 billion, with only 10% of drugs successfully reaching the market. Today, AI supports various stages of drug discovery and testing, accelerating the design, research, and trial phases, and making these processes more efficient and cost-effective (Daley, 2024).

AI is also utilized in digital medical communication, such as sending reminders and suggesting next steps of care to patients. These innovations improve the speed and accuracy of medical appointments, providing patients with smoother and more efficient access to diagnoses. This capability allows hospitals, clinics, and physicians to care for a larger number of patients daily. In the past, surgical robots operated under a “master-slave” system, meaning they lacked autonomous functionality and required human operators for control. However, advancements in AI have expanded the capabilities of surgical robots, enabling them to perform procedures autonomously. These AI-powered surgical robots rely

on sensor data and imaging to execute operations, enhancing the speed and precision of treatments without direct human intervention (Knudsen et al., 2024, p. 102). The application of AI in medical communication and robotic surgery exemplifies its potential to revolutionize patient care, increasing accessibility and efficiency in healthcare systems.

Nevertheless, the deployment of these technologies requires robust ethical frameworks and safeguards to ensure patient safety, equitable access, and the protection of sensitive medical data. AI's integration into healthcare not only enhances the precision and efficiency of medical practices but also addresses longstanding challenges in drug development, paving the way for more accessible and innovative medical solutions. However, as AI becomes more deeply embedded in healthcare, ethical considerations and regulatory measures are essential to ensure its equitable and safe application, particularly in safeguarding patient rights and data privacy.

The use of AI in healthcare services has sparked debates regarding labour rights, as outlined in Article 23 of the Universal Declaration of Human Rights (UDHR), Article 6 of the International Covenant on Economic, Social and Cultural Rights (ICESCR), and Article 15 of the

European Convention on Human Rights (ECHR). Critics argue that the drawbacks may outweigh the benefits in certain cases, particularly regarding employment. The replacement of healthcare workers, such as nutritionists and physiotherapists, by AI systems poses a significant risk of increasing unemployment in these fields. AI has demonstrated the ability to perform tasks such as nutrition planning and physical therapy programs, which may diminish the need for human professionals.

Moreover, the deployment of AI in healthcare raises concerns about privacy rights, as guaranteed by Article 12 of the UDHR and Article 8 of the Charter of Fundamental Rights of the European Union (CFR). AI systems often collect, store, and process sensitive and complex medical data, such as blood cell counts and hemoglobin levels. While these capabilities improve diagnostic and treatment precision, the storage and handling of such personal medical data come with risks. Data breaches or leaks could result in the misuse of this information by malicious actors, compromising patient safety and privacy. These concerns underscore the importance of balancing AI's benefits with its ethical and social implications. Safeguards must be in place to protect the labour rights of healthcare professionals and ensure that their roles remain integral within the

industry. Additionally, robust data protection measures and stringent regulatory oversight are essential to prevent privacy violations and misuse of sensitive patient information in AI-driven healthcare systems.

In cases of misdiagnosis by AI, despite its high efficiency in certain areas compared to human capabilities, errors can still occur, potentially leading to harmful outcomes. Addressing legal liability for such errors and compensating affected individuals is a complex issue, as AI currently lacks a legal status similar to that of humans. This situation raises concerns about fundamental human rights violations, particularly the right to life and personal security, as outlined in Articles 3 and 24 of the Universal Declaration of Human Rights (UDHR), Article 6 of the International Covenant on Civil and Political Rights (ICCPR), and Article 2 of the European Convention on Human Rights (ECHR). Misdiagnoses can jeopardize a person's life and safety, directly conflicting with these protections. Additionally, errors in healthcare diagnosis affect the right to access healthcare services, protected under Articles 4 and 35 of the Charter of Fundamental Rights of the European Union (CFR), and the right to rest and leisure, as stated in Article 12 of the International Covenant on Economic, Social and Cultural Rights (ICESCR). Patients suffering from

erroneous diagnoses may experience prolonged illness or worsening conditions, depriving them of their right to timely and effective medical care. Furthermore, legal accountability for such cases often falls into a grey area, leading to violations of the right to a fair trial and effective remedies, as guaranteed by Article 10 of the UDHR, Article 14 of the ICCPR, Articles 6 and 13 of the ECHR, and Article 47 of the CFR.

1.6 Law Enforcement by State Officials

AI has been increasingly utilized by law enforcement agencies, particularly in investigative work, where it can enhance security capabilities beyond those of human officers. However, the use of AI in this context raises significant concerns, especially regarding its impact on fundamental rights when applied by state authorities. One notable application is facial and voice recognition technology, which has advanced to the point where it can estimate an individual's age, race, and gender based on facial expressions. While these capabilities improve identification accuracy, they also risk infringing on the right to privacy, as enshrined in Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 8 of the Charter of Fundamental Rights of the European Union (CFR).

Another contentious use of AI is in predictive policing, a practice widely adopted in countries like the United States. Predictive policing employs algorithms to collect, process, and evaluate personal data related to past crimes to identify potential suspects or criminal activity. While this technology aims to prevent crime and enhance security, it has been linked to reports of rights violations, particularly regarding the collection and use of personal data. It may disproportionately target certain individuals or communities based on biased historical data, leading to discriminatory practices. The use of predictive policing raises fundamental concerns about fairness and non-discrimination, which are protected under Article 2 of the UDHR, Article 21 of the CFR, and Article 14 of the European Convention on Human Rights (ECHR).

Profiling individuals based on data-driven predictions, especially when the data is biased or incomplete, risks perpetuating systemic discrimination against marginalized groups. Furthermore, the lack of transparency in AI algorithms used for law enforcement can hinder accountability, complicating efforts to ensure justice and redress for affected individuals. These concerns emphasize the need for robust regulatory frameworks to govern the use of AI in law enforcement,

balancing security advancements with the protection of fundamental rights. Such frameworks should ensure transparency, accountability, and safeguards against misuse or abuse of AI technologies in this sensitive domain.

The use of predictive policing can lead to violations of rights related to discrimination, as individuals identified by such systems may face consequences such as constant surveillance by law enforcement agencies, even if they are innocent or wrongly flagged due to algorithmic errors. An example of this is the “Beware” program used by the Fresno Police Department in California. This program has been cited as a negative example of over-reliance on AI in law enforcement, highlighting its potential for misuse (Zakaria, 2023, pp. 233-257). Technologies like facial and voice recognition systems analyze facial and vocal features to predict criminal behavior. However, this capability often results in inaccurate predictions, misidentifications, or pre-emptive arrests of individuals who had no intention of committing a crime. For example, AI Live Facial Recognition (LFR) technology used by the Metropolitan Police in the United Kingdom linked CCTV cameras to a database of facial images. Reports revealed an accuracy rate of just 19%, meaning that the majority of individuals flagged as

suspects were, in fact, innocent (Dodd, 2022).

Another notable case is that of Randal Quran Reid in the United States. Reid was mistakenly identified by AI facial recognition while driving to his mother’s house on Thanksgiving. This misidentification led to his arrest and detention, as law enforcement incorrectly believed he was involved in a crime committed in Louisiana the previous month (Thanawala, 2023). These examples illustrate the dangers of over-relying on predictive policing technologies and facial recognition systems, particularly when such systems are prone to inaccuracies or biases. The wrongful identification of individuals violates fundamental rights, such as the right to non-discrimination under Article 2 of the Universal Declaration of Human Rights (UDHR), Article 21 of the Charter of Fundamental Rights of the European Union (CFR), and Article 14 of the European Convention on Human Rights (ECHR). Furthermore, such practices can undermine the right to a fair trial and the presumption of innocence, key principles of justice enshrined in international human rights law. These cases emphasize the urgent need for stricter regulations, transparency, and accountability in the deployment of AI in law enforcement. Governments and institutions must ensure that these

technologies are used ethically, without compromising fundamental rights or perpetuating systemic biases.

AI technologies, such as gunshot detection systems and DNA analysis, are widely used in law enforcement to enhance public safety and efficiency, but they can also raise significant concerns about human rights violations. The ShotSpotter system, a gunshot detection technology that employs sound sensors in key urban areas, has been extensively deployed across major cities in the United States; however, its limitations have led to controversies. A notable example is the case of Michael Williams, who was incarcerated for one year based on evidence derived from the ShotSpotter system, which was later deemed insufficient by prosecutors, leading to the dismissal of his murder charges (Independence, 2022). AI-driven DNA analysis processes using biological materials such as blood, saliva, semen, and skin cells, which can be transferred through contact between individuals or objects during a crime, have advanced significantly in sensitivity. These advancements enable the detection of minimal DNA quantities and the identification of genetic information from multiple contributors, even at extremely low concentrations. However, the use of such highly sensitive AI techniques may result

in the identification of DNA from multiple individuals, including those unrelated to the crime, potentially leading to errors.

AI technologies, including predictive policing, gunshot detection, and DNA analysis, can negatively impact fundamental rights. These include the right to freedom from discrimination, as protected by Article 2 of the Universal Declaration of Human Rights (UDHR), Article 14 of the European Convention on Human Rights (ECHR), and Article 21 of the Charter of Fundamental Rights of the European Union (CFR); the right to life, personal security, and human dignity, outlined in Articles 3, 4, and 22 of the UDHR, Articles 6 and 9 of the International Covenant on Civil and Political Rights (ICCPR), Articles 2 and 5 of the ECHR, and Articles 1-3 and 34 of the CFR; the freedom from torture, arbitrary arrest, and cruel treatment, as guaranteed by Articles 4, 5, and 9 of the UDHR, Articles 7, 8, 10, and 11 of the ICCPR, Article 3 of the ECHR, and Article 4 of the CFR; and the right to be presumed innocent until proven guilty, equality before the law, fair trials, and access to justice, as enshrined in Articles 6-8 and 10 of the UDHR, Articles 14-17 and 26 of the ICCPR, Articles 6 and 7 of the ECHR, and Article 20 of the CFR.

The use of AI in political and democratic processes has also been found

to have negative impacts. Political and democratic information disseminated by AI can influence individuals who do not regularly follow the news, lack clear political beliefs, or possess limited political knowledge. These individuals often rely on accessible information sources or online media to understand the situation. Consequently, the creation of false information by AI—whether in the form of text, images, videos, or audio—can lead people to believe and accept misleading narratives about political opinions and democratic expression. In such cases, the right to freedom of opinion and expression, as protected by Article 19 of the Universal Declaration of Human Rights (UDHR), Article 11 of the Charter of Fundamental Rights of the European Union (CFR), and Article 10 of the European Convention on Human Rights (ECHR), is directly affected.

In electoral processes, such as predictive technologies for opinion polling, AI can significantly impact the political identity and interests of voters during elections. A notable example is the events preceding the 2016 United States presidential election, where the dissemination of false information supported by algorithms affected the personal data of Facebook users and influenced their voting behaviour (Bakiner, 2023). Additionally, the mobilization of

individuals both online and offline, driven by misinformation and conspiracy theories, poses risks to the integrity of public discourse and undermines trust among individuals in democratic societies. This affects the right to political participation, as outlined in Article 15 of the International Covenant on Civil and Political Rights (ICCPR), and the right to vote, as enshrined in Articles 39 and 40 of the Charter of Fundamental Rights of the European Union (CFR).

2. The EU AI Act and Its Provisions Regarding the Protection of Fundamental Rights

In terms of fundamental rights protection, the world's first regulation for AI was enacted in the European Union as the European Artificial Intelligence Act 2024, also known as the EU AI Act (Regulation (EU) 2024/1689), which came into effect on August 1, 2024. This legislation consists of 13 chapters and 113 articles. The adopted legislation clearly defines the primary objective of the EU AI Act in Article 1, stating: "The purpose of this Regulation is to... ensuring a high level of protection of health, safety, and fundamental rights enshrined in the Charter..." (European Union, 2024). This affirms that fundamental rights will be protected at a high level against the use of AI.

Moreover, the EU AI Act classifies AI technologies into four primary categories, determined by the potential risks associated with the AI system. These categories include (European Commission, 2025):

(1) Unacceptable Risk: All AI systems identified in this category are deemed a significant threat to the safety, livelihoods, and rights of individuals and are therefore prohibited. Instances of unacceptable-risk AI systems encompass harmful AI-driven manipulation and deception, exploitative use of vulnerabilities through AI, social scoring, risk assessment or prediction of individual criminal offenses, indiscriminate scraping of the internet or CCTV footage to develop or enhance facial recognition databases, and real-time remote biometric identification for law enforcement in publicly accessible areas.

(2) High Risk: According to Article 6 of the EU AI Act, high-risk AI systems are defined as those that present a considerable threat to health, safety, or fundamental rights. These systems are categorized into two primary groups. First, AI systems that are incorporated into or form part of products governed by current EU harmonization legislation. Second, AI systems employed in particular high-risk applications specified in Annex III of the AI Act. Instances of AI systems within this risk-oriented framework include the

following: AI safety mechanisms in critical infrastructures (such as transportation), whose malfunction could jeopardize the lives and health of citizens; AI applications employed in educational institutions, which may influence access to education and the trajectory of an individual's professional career (for instance, exam scoring); AI-driven safety features in products (for example, the application of AI in robot-assisted surgical procedures); AI instruments for employment, workforce management, and self-employment opportunities (such as CV-sorting software utilized in recruitment); Specific AI applications designed to facilitate access to vital private and public services (for example, credit scoring that may prevent citizens from securing loans); AI systems implemented for remote biometric identification, emotion detection, and biometric classification (such as an AI system used to retroactively identify shoplifters); AI applications in law enforcement that could infringe upon individuals' fundamental rights (for example, assessing the reliability of evidence); AI applications in migration, asylum, and border control management (such as the automated review of visa applications); and AI solutions employed in the administration of justice and democratic processes (for instance, AI systems used to draft court rulings).

(3) Limited Risk: This classification encompasses AI systems that engage directly with individuals yet do not present considerable dangers. Examples include chatbots and virtual assistants – AI-enhanced customer service bots, like those employed by financial institutions or online retail platforms; deepfake content creation – AI-produced images, audio, or video must be distinctly marked as synthetic; and AI-based recommendation systems – such as those utilized by streaming services or e-commerce platforms.

(4) Minimal Risk: Examples of this system include spam filters – AI systems designed to identify and eliminate unwanted emails; AI-driven video game adversaries – non-player characters in video games that respond to player actions; and elementary recommendation systems – AI that proposes music, films, or articles tailored to user preferences.

The purpose of this classification is to clearly establish criteria for determining which types of AI must be subject to which specific conditions for the protection of fundamental rights before being deployed. A high-risk AI system is required to complete several conditions. For example, providers of this AI application must implement risk management systems (Article 9), to identify and mitigate risks across the AI system lifecycle. Transparency, record keeping,

data governance, and documentation (Articles 10-13) are responsible for maintaining thorough documentation on system functionality, data sources, and decision-making processes. Article 15 states that providers need to design high-risk systems with security-by-design, ensuring accuracy, resilience, and cybersecurity. Moreover, providers listed in Annex III, must conduct a conformity assessment—internally or via a notified body—to verify compliance, as illustrated in Articles 31 and 43. For Deployers, Article 14 sets the criteria called human oversight, which the deployers of the high-risk AI system must establish mechanisms to allow human intervention, enabling users to oversee and intervene in AI decisions as needed. Failure to comply with these conditions may result in penalties, such as fines or other sanctions.

Limited and minimal-risk AI systems encounter few regulatory requirements. Typically, these systems operate without regulation, except in instances where transparency obligations are mandated. In general, these two categories of systems are required to ensure transparency and provide clear disclosures (developers and deployers must notify users that they are engaging with an AI system). This can be achieved through explicit notifications or labelling. Certain AI systems deemed to

present limited or minimal risk are still required to be registered in the EU database in accordance with Article 71. Minimal-risk AI systems must adhere to best practices, particularly when mandated by other regulations, such as safeguarding data privacy and addressing biases in AI algorithms to promote fair and impartial outcomes.

The EU AI Act outlines a framework that can be utilized by other regions and nations as a reference for developing their domestic and regional policies and regulatory structures. This Act represents one of the legal mechanisms established by the EU to oversee and regulate specific contemporary issues, particularly those related to artificial intelligence. It delineates the roles of various authorities at both the regional and national levels. Chapter VII specifies the establishment of an AI officer within the Union. Articles 65-66 indicate that the European Artificial Intelligence Board (the Board) will consist of one representative from each member state, tasked with advising and assisting the EU Commission and the member states. Article 67 details the formation of an advisory forum that will provide technical expertise and guidance to both the Board and the EU Commission, contributing to their responsibilities. Furthermore, Article 68 mandates the creation of a scientific panel

of independent experts, referred to as the ‘scientific panel,’ which is intended to support enforcement activities under the EU AI Act. Each member state is also required to establish national competent authorities, including at least one notifying authority and one market surveillance authority, to exercise their powers independently, impartially, and without bias, as stipulated in Article 70.

■ Conclusion and Recommendations

In conclusion, the findings of this research can be summarized by stating that AI can cause negative impacts and infringe on fundamental rights, guaranteed by the five major international human rights conventions. This study has highlighted several areas in which AI can have adverse impacts on the daily lives of individuals, divided into six categories: (1) Use of online service platforms; (2) Transportation and logistics; (3) Financial services; (4) Education and human resources; (5) Healthcare; and (6) Law enforcement by state authorities. From the illustration of adverse impacts, it is concerning that undesirable effects may arise in the future with the use of AI, requiring the development of policies or laws to protect fundamental rights, as measures based on existing

international human rights laws do not specifically address the negative consequences caused by AI. Therefore, this research recommends the development of guidelines for the prevention and protection of rights that may be affected by the use of AI, drawing on the approach of the European Union (EU), which has put in place new legislation specifically aimed at protecting against the impacts of AI, while focusing on safeguarding fundamental rights. Thus, the European Union's Artificial Intelligence Act can be recommended as a model for other countries and regions wishing to develop additional legal frameworks and also policies for AI. However, this study does not advocate relying exclusively on the EU AI Regulation as a reference.

Eventually, this research outlines the suggestions for Future Research as follows.

(1) Study the negative impacts of AI from other perspectives beyond the six dimensions defined in this research.

(2) Investigate approaches to prevent violations of fundamental rights due to the use of AI in other countries such as the United States, the United Kingdom, Australia, or ASEAN member states, in order to compare policies and laws. The focus should be on the important issues that the state must play a crucial role in protecting citizens' rights from violations caused by

the use of AI. The state should enact laws or establish effective policies regarding the management, support, and regulation of AI usage.

(3) Determine the circumstances under which human rights protection entities, whether at the national, regional, or global levels, ought to engage with AI users and developers, and investigate the associated mechanisms and responsibilities. In this context, it is advisable to examine the current mechanisms and legal frameworks pertinent to this issue. For instance, within the EU, the European Court of Human Rights can fulfill its function as an effective mechanism for safeguarding fundamental rights that are infringed upon by AI technology. Furthermore, the compensation process for victims whose rights are jeopardized by the use of AI will be organized, overseen, and rectified.

(4) Examine the role of the private sector in innovating and implementing AI, specifically how private entities develop models and manage risks associated with AI in alignment with state policies and laws. What regulatory measures or obligations should be imposed on the private sector? At the same time, it is essential to study and understand the scope of state obligations when using AI systems developed by the private sector, while also promoting technological development alongside

private sector producers and service providers of AI.

(5) Study the role of civil society in the development of policies and laws related to AI, including participation in advocacy and providing observations to monitor the impacts, advantages, and disadvantages that may arise, as seen from the perspective of civil society.

References

- Adwan, A. & Aladwan, R. (2022). Use of artificial intelligence system to predict consumers' behaviors. *International Journal of Data and Network Science*, 6(4), 1223-1232. <https://doi.org/10.5267/j.ijdns.2022.6.011>
- Bakiner, O. (2023). The promises and challenges of addressing artificial intelligence with human rights. *Big Data & Society*, 10(2). <https://doi.org/10.1177/20539517231205476>
- Black, J. (2023). Past, present and tackling the future of artificial intelligence (AI) in education: Maintaining agency and establishing AI laws. *Open Journal of Social Sciences*, 11(7), 442-464. <https://doi.org/10.4236/jss.2023.117031>
- Carvalho, I. & Ivanov, S. (2024). ChatGPT for tourism: Applications, benefits and risks. *Tourism Review*, 79(2), 290-303. <https://doi.org/10.1108/TR-02-2023-0088>
- Chakraborty, C. & Joseph, A. (2017). Machine learning at central banks. *Bank of England Staff Working Paper No. 674*. <https://doi.org/10.2139/ssrn.3031796>
- Cordeschi, R. (2007). AI turns fifty: Revisiting its origins. *Applied Artificial Intelligence*, 21(4-5), 259-279. <https://doi.org/10.1080/08839510701252304>
- Costa, E. B., Fonseca, B., Santana, M. A., Araújo, F. F. D., & Rego, J. (2017). Evaluating the effectiveness of educational data mining techniques for early prediction of students' academic failure in introductory programming courses. *Computers in Human Behavior*, 73, 247-256. <https://doi.org/10.1016/j.chb.2017.01.047>
- Curtis, N. (2023). To ChatGPT or not to ChatGPT? The impact of artificial intelligence on academic publishing. *Pediatric Infectious Disease Journal*, 42(4), 275. <https://doi.org/10.1097/INF.0000000000003852>
- Daley, S. (2024, June 14). *AI in healthcare: Uses, examples and benefits*. Built In. <https://builtin.com/artificial-intelligence/artificial-intelligence-healthcare>
- Dodd, V. (2022, October 27). *UK police use of live facial recognition unlawful and unethical, report finds*. The Guardian.

- <https://www.theguardian.com/technology/2022/oct/27/live-facial-recognition-police-study-uk>
- European Commission. (2025). *Shaping Europe's digital future: AI Act*. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending various regulations and directives (Artificial Intelligence Act)*. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- European Union Agency for Fundamental Rights (FRA). (2020). *Getting the future right – Artificial intelligence and fundamental rights*. <https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights>
- Gil De Zúñiga, H., Goyanes, M., & Durotoye, T. (2024). A scholarly definition of artificial intelligence (AI): Advancing AI as a conceptual framework in communication research. *Political Communication*, 41(2), 317-334. <https://doi.org/10.1080/10584609.2023.2290497>
- Gugerty, L. (2006). Newell and Simon's Logic Theorist: Historical background and impact on cognitive modeling. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 50(9), 880-884. <https://doi.org/10.1177/154193120605000904>
- Harrison, J. (2023). Human rights due diligence: Challenges of method, power and competition. *CHRIIP Working Paper Series*, 2023(2). School of Law, Coventry. <https://wrap.warwick.ac.uk/id/eprint/174876/>
- Independence. (2022, March 5). *Police jailed a man for murder; Algorithm was key evidence*. The Independent. <https://www.independent.co.uk/news/michael-williams-police-chicago-cook-county-jail-herring-b2029463.html>
- Jason. (2024). AI in eCommerce statistics (2025). *Sellers commerce*. <https://www.sellerscommerce.com/blog/ai-in-ecommerce-statistics/>
- Jungherr, A. (2023). Artificial intelligence and democracy: A conceptual framework. *Social Media + Society*, 9(3), 20563051231186353. <https://doi.org/10.1177/20563051231186353>
- Kaur, D., Sahdev, S. L., Sharma, D., & Siddiqui, L. (2020). Banking 4.0: The influence of artificial intelligence on the banking industry & how AI is changing the face of modern-day banks. *International Journal of Management*, 11(6), 577-585.

- Knudsen, J. E., Ghaffar, U., Ma, R., & Hung, A. J. (2024). Clinical applications of artificial intelligence in robotic surgery. *Journal of Robotic Surgery*, 18(1), 102. <https://doi.org/10.1007/s11701-024-01867-0>
- Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2017). ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, 60(6), 84-90. <https://doi.org/10.1145/3065386>
- Kubica, M. L. (2022). Autonomous vehicles and liability law. *The American Journal of Comparative Law*, 70(Supplement_1), i39-i69. <https://doi.org/10.1093/ajcl/avac015>
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444. <https://doi.org/10.1038/nature14539>
- Mittal, A., Chaturvedi, D. D., Chaturvedi, S., & Singh, P. K. (2024). Impact of Negative Aspects of Artificial Intelligence on Customer Purchase Intention: An Empirical Study of Online Retail Customers Towards AI-Enabled E-Retail Platforms. In S. Dadwal, S. Goyal, P. Kumar, & R. Verma (Eds.), *Demystifying the Dark Side of AI in Business* (pp. 159-173). IGI Global Scientific Publishing. <https://doi.org/10.4018/979-8-3693-0724-3.ch010>
- Pshychenko, D. (2024). Automation and optimization of logistics process using AI. *Sciences of Europe*, 145, 64-67. <https://doi.org/10.5281/zenodo.12910522>
- Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 4, 100005. <https://doi.org/10.1016/j.jrt.2020.100005>
- Roser, M. (2022, December 6). *The brief history of artificial intelligence: The world has changed fast — what might be next?* Our World in Data. <https://ourworldindata.org/brief-history-of-ai>
- Schrittwieser, J., Antonoglou, I., & Hubert, T. (2019). Mastering Atari, Go, Chess and Shogi by planning with a learned model. *arXiv reprint*. <https://doi.org/10.48550/ARXIV.1911.08265>
- Srinadi, N. L. P., Hermawan, D., & Jaya, A. A. N. A. (2023). Advancement of banking and financial services employing AI. *JoWUA*, 14(1), 106-117. <https://doi.org/10.58346/JOWUA.2023.11.009>
- Thanawala, S. (2023, September 25). *Facial recognition technology jailed a man for days*. AP News. <https://apnews.com/article/mistaken-arrests-facial-recognition-technology-lawsuits>
- Wang, S., Wang, F., Zhu, Z., Wang, J., Tran, T., & Du, Z. (2024). Artificial intelligence in education: A systematic literature

review. *Expert Systems with Applications*,
252, 124167. [https://doi.org/10.1016/
j.eswa.2024.124167](https://doi.org/10.1016/j.eswa.2024.124167)

Zakaria, M. G. (2023). AI applications in
the criminal justice system. *Journal of
Law and Emerging Technologies*, 3(2),
233-257. [https://doi.org/10.54873/
jolets.v3i2.124](https://doi.org/10.54873/jolets.v3i2.124)

Zhuang, K. V. & Goggin, G. (2024). New
possibilities or problems for disability
and inclusion? The case of AI and ADMs
across work. *Telematics and Informatics*,
92, 102156. [https://doi.org/10.1016/
j.tele.2024.102156](https://doi.org/10.1016/j.tele.2024.102156)



