ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد الثمانون
تاريخ الإصدار: 2 – حزيران – 2025م
www.ajsp.net

"The Role of Artificial Intelligence in Human Rights Violations and The Importance of AI Governance in Protecting Human Rights"

Researcher:

Dr. Ziad Zouheiry

International relation, CEDS (centre d'etudes diplomatiques et strategiques), Paris, France.

Oricd No: 0009-0004-1011-8931

https://doi.org/10.36571/ajsp803

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار الثامن – العدد الثمانون
تاريخ الإصدار: 2 – حزيران – 2025م
www.ajsp.net

Abstract:

Artificial intelligence (AI) systems is a new technology which is changing our lives, because, meanwhile, we can find AI in everything. For instance, AI technology exists in our phones, homes, cars, work, computers, hospitals and other places, and this is a critical issue, as AI technology is a double-edged sword and there are good side and bad side in AI technology, in this research we are focusing on the bad side specifically the bad effects of AI technology on human rights and ethics. Moreover, AI systems are considered a threat to privacy, data protection, the environment, unemployment rate, cyberwars, intellectual property and others. Besides, there were a lot of unsuccessful attempts from all countries around the world to create regulations for the AI technology, such as the Paris summit, and this failure led us to propose AI governance as the official regulation for AI technology Also in this research, we used the mixed methods (quantitative and qualitative methods) in collecting our data, and our data resources were reliable and credible based on our criteria of credibility, likewise we used the inductive reasoning in our research.

Keywords: AI technology, AI governance, cyber war, environment, Human rights violations, ethics.

1-Introduction:

Artificial intelligence is the invention of this century which is changing the traditional image and the culture of the world. Without any doubt, AI is positively affecting our lives, and we can now find AI technology in everything, starting with our smart home, and our smart cars, which can be driven by auto drivers. Besides, most jobs, meanwhile, are counting heavily on AI systems that can achieve many important job tasks, even the hospitals are replacing human nurses with robots:" the worldwide robotic nursing industry is expected to grow 17.07% by 2031." (Falcon, n.d.)

The relationship between AI systems and human rights remains vague, and the AI is a double-edged sword as it has a positive and a negative side and here we will focus on the negative side, specifically that AI is a major component in cyber-attacks, and the international organizations such as the UN (UNESCO, n.d.) and EU (European Parliament, n.d.) concern about the consequences of the AI deployment in the society for that reason those organizations created guidelines and recommendations related to AI which include data protection, privacy, discrimination, but they did not cover the human rights violations resulted from the bad effects of AI on unemployment rate and wars, also the AI has a critical consequence on environment as like global warming, energy consumption, and scarcity of water.

In this research we will mention most the AI human rights violations and the AI's critical leverage on environment and wars.

1.1Data protection:

AI is an algorithm function and AI data gathering is the responsibility of the user of this function, and sometimes the data is personal data, which includes personal identity, race, ethnicity, interests and opinions.

Those kinds of data may violate human rights if they are transferred to a third party without consent, as like data mining firms who pretend that this personal data can help to invent a system of justice that can detect and investigate criminals but according to Rebecca Wexler:" Many of these technologies are opaque, have low accuracy rate and can perpetuate discriminatory practices. One can therefore question whether the sweeping deployment of AI enhances or rather compromises effective protection of the right to liberty and security" (Wexler, 2018) For that reason, there must be agreement before any data transfer and the process must be made with high accuracy to avoid violations of human rights. At the business level, some companies during the COVID epidemic were obliged to work from a distance and some employees used their phones in their online meetings, which was risky to the privacy of their businesses, because most of the smartphones contain Alexa that can result in business information leakage (Sloan, n.d.). Besides, the companies obliged their employees to turn off the Alexa option for data protection purposes.

Hackers can easily attack a program of facial recognition technology (FTR) if the data is not technically secured enough or the data is not encrypted and the FTR is" at the forefront of surveillance technology fueled by AI that is changing the laws of enforcement across the globe." (Ferguson, 2021)

This kind of attack can disclose the face print of the person, which is a human rights violation, because the attackers are breaking the secrecy, intimacy and the personal information of the individual.

Furthermore, many ring home security cameras, which are controlled by AI in four different states in the USA, were breached by hackers because of the weak security code of the surveillance system. Cybersecurity experts say it is not that difficult for hackers to gain access to Internet of Things devices, which include ring security cameras and voice assistants, such as Alexa and Google Home. (Vidgor, n.d.)

Those attacks proved that some AI systems like Alexa and Google Home are not efficient enough for the data protection of people, but it is always the responsibility of the programmer. Besides, there are some AI programs that can perform independently of the developer, and those programs can make unexplainable decisions even though the programmers cannot explain the way of making the decision. This situation is called the black box phenomenon (Rawashdeh, n.d.) and that leads to a problem of accountability and transparency, which are fundamental in Data protection:" The opacity of AI models has led some to argue that legal accountability mechanisms are not sufficiently developed to keep pace with AI" (Crawford, 2018).

1.2 Privacy:

The right to privacy in AI systems is the right of people to limit access to the use of personal information related to them, and the right to privacy is mentioned in article 12 of the Universal Declaration of Human Rights (UDHR) and in article 7 of the European Union EU charter of fundamental Rights.
Unfortunately, many governments maliciously use AI technology such as surveillance cameras (CCTV) with the option of FRT (facial recognition technology) to illegally monitor their civilians, which is a violation of the privacy of their citizens (Feldstein, n.d.).
For instance, China has installed a network of more than 626 million FRT cameras all across the country (Jacque, 2021) for legal purposes, but there are many rumors which say that the FRT cameras were deployed to monitor and record the facial signatures of the Uygur Muslims:" there are concerns regarding increasingly the intrusive nature of FRT surveillance exemplified by the allegation of profiling of Uygur Muslims." (Mauzur, n.d.)
This kind of profiling breaks the privacy of the monitored person, and it is illegal to use the FRT camera for unlawful purposes and this phenomenon is called function creep:" the expansion of a technological system beyond its original and proper purpose" (Koops).
The privacy and liberty rights are violated in Africa also, because China is also the main exporter of the FRT camera technology to Africa, and in 2020 the Chinese companies exported to Uganda the system of FRT cameras and this led to the arrest of more than 836 civilians in protest:" by utilizing a network of CCTV cameras supplied by the Chinese company Huwai, raising concerns that the Uganda authorities were accessing the system for conducting FRT enhanced surveillance of those opposed to the incumbent regime." (Kafeero, n.d.)
Many people around the world have protested against the misuse of FRT cameras, which breaches the privacy of people, as what happened in Hong Kong in 2019-2020:" Protesters responded to these risks by wearing face masks, carrying umbrellas and destroying surveillance towers, leading the government to ban facial covering." (Millet, n.d.)
AI spyware attacks are a big threat to the privacy of people, since this malware can easily steal the credentials and the personal information of people from their personal computers. Also, this kind of AI malware is a very sophisticated version of malware that can simply penetrate any target without being noticed by the security system, because there is no technology till now that can defend itself from this AI spyware.
Besides, cybercriminals are counting on AI systems in their phishing attacks, which are increasing noticeably by tricking their victims into sharing their personal information." AI systems have made it easier for cybercriminals to carry out phishing messages, mimicking people's voices researching targets and creating deepfakes, also the IT leaders are witnessing AI-powered attacks increase at the rate of 51% ." (D'andrea, n.d.)

1.3 Discrimination:

Many AI applications contain biased data concerning race, sex and color, which is a very dangerous thing in society:" an increased focus on racial discrimination in the application of these technologies and the extent to which these technologies entrench existing inequalities" (Borgesius, 2020). And discrimination is prohibited in article 2 of the human rights

declaration. Lately, many accidents related to discrimination have happened because of the extensive reliance on AI applications which contain unreliable data on people of color (Belenguer, 2022).
For instance, the AI in Google created a folder called gorilla which contains photos of black people. (Metz, n.d.)
Another accident related to the criminal justice system happened in the USA, when an African American man was arrested mistakenly for shoplifting because the police officer depended on facial recognition technology and the AI was not functioning properly since the tool had not learned how to recognize the faces of black people. (UN News, n.d.)
Besides, the courts in the USA are using, right now, an AI system named COMPAS (correlation offender management profiling for alternative sanctions) and the system assesses the probability of a person reoffending a crime and the system can suggest the suitable sentence for the criminality that was practiced by this specific person, but according to Lel Jones:" the technology is meant to reduce bias in law enforcement, but instead, it reinforces stereotypes of people of color being repeated offenders." (Jones, 2020)

1.4 Unemployment:

In the economic history of technology there has always been a negative relationship between the unemployment rate and the new innovations of technology. The historian Ben Schneider declared that the mechanization of hand spinning had negatively affected the wealth of women and their families in seventeen centuries:" In the 1770s, hand spinning provided for more than eight percent of the population, primarily women, the loss of this home-based work as a result of the mechanization commencing in the 1780s and persisting for a half century." (Schenieder, n.d.)

Another example in the history of the mechanization which is similar to AI is the mechanization of telephone switch board, as in 1920 more than 300,000 people were Employed in the telephone switch board sector, but after the creation of the mechanization more than 80 percent of the employees lost their jobs. (Gross, n.d.)
There are studies proving that the excessive deployment of robots in the future will lengthen the unemployment duration, especially for workers in routine occupations and for unskilled workers (Wan, 2025).
AI is indirectly affecting the incomes of people and this is a human rights violation, according to article 23 in the human rights declaration, which is about Everyone has the right to work, the right to equal pay for equal work.

1.5 The wealth:

Article 17 of the universal human rights declaration forbids depriving arbitrary others of their own property and property can mean money and wealth.
Lately, AI has been utilized intensively by cybercriminals in fabricating ransomware, which is a big business for cyber attackers, who were paid more than $1 billion in ransom in 2023. (Delman, n.d.)
By installing the AI technology in ransomware, criminals can increase the level of damaging functionality and the level of sophistication with which the ransomware can be invisible for detection and faster in spreading also with higher financial gains.
Moreover, the deepfake software created by the AI is another tool which is used by hackers to steal money from innocent people. In 2024, an employee of a UK engineering company transferred $25 million to cybercriminals after talking to his manager via video call. The video call was a deepfake created by artificial intelligence, and this was a new kind of cybercrime that consists of a combination of psychological manipulation and deepfake technology to convince the employee that the operation is true. (Eliott, n.d.)

1.6 AI and environment:

Meanwhile, The AI is used excessively by people and around 300 million users are using the CHATGPT weekly, and the CHATGPT is chat bot-based system requires a huge database which contains a large language models, text and images in order to generate new content.

For instance, every person who ask the CHATGPT for a task, it needs about 3W per hour for energy and this is according to the international energy agency (You, n.d.), also the amount of energy that is consumed daily by AI data center can charge more than 3 million electric cars.

The AI systems have a lot of data centers and the number of AI data centers are uncountable and they consume about 1.5% (Chen, n.d.) of global electricity usage as with one single data center's consumption per year we can power electricity for more than 50,000 homes yearly.

Besides the experts are afraid that the consumptions are going to increase in the next year because there are countries like Japan and Russia in which the number of AI data centers Are extending gradually and this will increase the electricity demand globally, which will put additional strains on electricity grids.

Normally, in data centers, they use air-cooling systems to decrease the rising temperature resulting from the overheating emitted from the data servers, but this system is not effective for AI technology. Right now, most of the AI data centers are using a liquid cooling system, which depends mainly on water to preserve the ideal temperature of 21 to 24 degrees Celsius. Furthermore, researchers from the USA predict that by 2027, 6.6 billion cubic meters of water (Gordon, n.d.) will be needed to satisfy global demands and this is equivalent to half of the UK's water consumption per year.

Another point to discuss AI's effects is the rise in greenhouse gas emissions around the globe and this is a main cause of global warming, but there is still no clear figure about AI's contribution to global emissions.

Furthermore, the international energy agency estimates that data centers account for 0.6% of annual emissions (singh, n.d.), and the organization of science and technology in Australia admits that the result is 1% (htt2). Recent reports claim that if AI adoption continues to grow, there is a great possibility that by 2040, the data centers will be 14% of the yearly emissions sources. For example, Microsoft has had a 30% increase in its carbon emissions since 2020 because of the AI models and services that Microsoft offers, and until now this tech giant has no plan to reduce the emissions, which means that there will be extra demands for its resources and infrastructure in the future.

Moreover, mineral resources are going to decrease as a result of high AI technology adoption, specifically lithium, which is one of the main minerals that is used to produce the rechargeable batteries that power the AI technology, and Australia is the largest producer of this mineral. Also, it is estimated that lithium is going to disappear within the next 75 years due to the high demand for AI services.

As we can see that the high utilization of AI technology is leading us to many critical problems, such as global warming because of the emissions produced by data centers, and this is harming our ecosystem a lot, and it is killing our animals and threatening humans 'lives and this unethical, also it is environmental right violation, besides the water scarcity is recognized by the UN as a human rights violation:" fundamental to everyone's health, dignity and prosperity." (Dhanabalan Thangam& M, n.d.)

Additionally, the extensive use of lithium is leading us to human rights violations since the mining process may cause many problems for the environment and for the human beings, and historically the mining had caused a high rate of pollution and people who lived near The mining locations suffered from health problems. For that reason, the UN declared article 25, which states that:" Everyone has the right to live to a standard of living adequate for the health and wellbeing (Bashkaran, n.d.) of himself and of his family."

1.7 AI and Wars:

Most of the powerful armies are changing their traditional military strategies on the battlefields because of AI, since AI helps commanders to have accurate images and information about the battlefield in a short time from the central command center, as the AI systems can collect data and images related to the enemy from the electro-optical sensors on a satellite and AI sends them back to a central command center where the decision is made, also the AI command center is armed with computer vision software that is processing all of this incoming visual data, and the software can automatically look over those images and information, and the AI fuses all the data together, and it starts to make predictions and inferences, and it gives recommendation to the commander with 90% probability of success, besides the AI could recommend drones for the attack which are automated and can fly solely without human control and the drones can hit target without human instructions depending on their precision guidance.

Moreover, the relationship between AI and ethics remains unclear, according to Dr. Shwarz:" The integration of AI-enabled weapon systems facilitates the objection of human targets, leading to heightened tolerance for collateral damage" (Shwarz, n.d.), which means that the AI doesn't mind killing innocent people in order to achieve its main objective on a battlefield and this is unethical because it is considered a discrimination act against the civilians, also it does not respect the proportionality principle in war ethics which prohibits killing or harming civilians during attacks against military objectives. Additionally, we cannot predict the response of AI if we give it more information and more decisions ability. For example, it could get out of control and this is a catastrophe as the AI can cause war easily and rapidly.

1.8 AI and intellectual properties:

An AI system such as CHATGPT is supported with data that includes books, images and articles and this huge quantity of data may contain copyrighted sources which can violate intellectual property rights and this is what happened with a company called Getty Images:" visual media company called Getty Images accused stability AI Inc. of using more than 12 million photos without permission and compensation." (Ridhhi Setti, n.d.), also the AI can produce a text which is similar in content to other copyrighted text and this is what happened in the tech news site CNET:" CNET's AI appears to have been a serial of plagiarist of actual human's work." (Prowriters, n.d.) Furthermore, the universal declaration of Human rights declared in article 27 the right to intellectual property:" everyone has a right to the protection of moral and material interests resulting from the authorship of scientific, literary, or artistic production" (Laws, n.d.)

1.9 AI Resolutions:

The first official treaty about AI is the AI Council of Europe treaty, which ensures the protection of human rights, rule of law and legal standards:" The treaty includes a number of key concepts from the EU, such as risk-based approach, transparency along the value of AI systems and AI generated content, detailed documentation obligations for AI systems for identified as high risk. (Council of Europe, n.d.) But the problem of this treaty that it was limited because the treaty does not cover all the possible risks resulted from the AI as like unemployment risk, environment risk, intellectual property risk, and cyberwar risk, also legally the treaties execute very few restrictions:" it is sometimes arguing that treaties too rigid and slow to be useful for effective global governance." (Global AI governance, n.d.) And there are many examples of fragile treaties that had happened in the past and most of the bottlenecks in treaties' negotiations are related to domestic politics but not international law.

In 2025, there were a summit in Paris (Joshi, n.d.) about the global governance of AI, and the main purpose of this summit was to establish effective international cooperation among countries to produce AI governance. Also, the summit was interested in:" creating sustainable ecosystems, especially for creative industries and establishing scientific consensus on AI safety and security" (Jacque, 2021). The summit failed because the USA and the UK refused to sign the statement because both countries were afraid that extreme regulations on AI governance could negatively affect innovation in the AI sector. (Science and Technology, n.d.)
Moreover, China declared in 2023 its measures for the management of generative artificial intelligence services, and according to the Chinese measurement, the users of AI services must respect the human rights:" it is required to not endanger the physical and mental health of others, and do not infringe upon other's portrait rights, reputation rights, honor rights, privacy rights and personal information rights." (Aljazeera, n.d.)

Besides, there is great interference between AI and cyber-attacks, since most cyber criminals are using AI systems to create malware as we mentioned earlier. Also, most of the cyberwars depend heavily on AI technology, like drones and central command centers, which means that AI is an important part of cyberwarfare. For that reason, the Tallinn manual was created with the support of NATO to protect civilians from cyber-attacks during warfare. Also, Tallinn inspects the international law governing cyber warfare,
But all the cyber activities which happen beneath the level of use of force, like AI cyber criminalities, have not been coded in the manual. Besides, the manual did not mention other fields of international law, such as human rights or telecommunication law.
Furthermore, the manual is far from the cybersecurity issue like cyber espionage and theft of intellectual property, which are not addressed in the manual (Schmitt, 2013).
The aim of this study is to find a way to limit the bad effects of AI on humanity, and we find that AI governance is the best solution to avoiding human rights violations and many other related problems.
Additionally, the large number of innocent people who were arrested randomly and the huge number of casualties because of the malpractice of AI was our main reason for conducting this research, which was based on many incidents that had happened in many countries.

2-Methodology:

The research article discusses the bad effects of AI technology on human rights and ethics and the role of AI governance in protecting those rights. In the research, we mentioned many examples of bad AI technology's consequences on human rights, such as data protection, privacy, discrimination, unemployment, wealth, intellectual property, cyberwars and the environment. Also, we wrote many AI tech resolutions, like the European Union treaty, Paris summit and the Chinese measurement of AI technology.

Furthermore, we used both the quantitative and qualitative methods in this research. For example, we used the quantitative method by putting many numbers and percentages in the research, especially in the sections of the environment, like the amount of electricity consumption by the AI data centers, and the amount of water consumed by the cooling systems in AI data centers, besides the percentage of AI technology in the production of greenhouse emissions and the quantitative method were very supportive of this research by showing the numbers which proved the critical consequences of AI technology on the environment, but the qualitative method was mainly used in the research, and I used the secondary research method, as the data in the research were based on many books such as Tallinn Manual, Artificial intelligence and human rights book and the industries of the future book, likewise I used many websites in the research like IBM, global AI governance, CSIS, Bloomberg, United Nations and University of Oxford, as well most of the data sources that I used in the research were based on my criteria of credibility as the data sources were relevant to my research topic, and they were credible because the authors of the books and articles are experts in their fields, also most of the data in the research were recently added which gave more credibility to my research.

Moreover, for my first research strategy, I consulted many sources for data collection, like the Google search engine, with which I found many articles and websites about the bad Effects of AI technology on human rights and others. Besides, I used Google Scholar to find journal articles which are similar to or contradict my research topic. For instance, I Downloaded many journal articles from indexed journals Likewise, I searched and downloaded many e-books from Amazon book stores.

My second research strategy is critical thinking, as first I identify the problem which was the bad effects of AI tech on ethics and human rights. Second, I collected a lot of information related to AI tech and human rights violations. Third, I analyzed the collected data on AI technology and human rights violations. Fourth, I consider other viewpoints. As we can see in the research, there are a lot of articles which contradict my opinion about the importance of AI governance. Fifth, I drew a solution to the problem, which was AI governance.

Furthermore, I used in the research many examples of the bad effects of AI technology. I also identified regularities to solve those problems. Then I reached a hypothesis, which was AI governance that can solve the bad consequences of AI technology on human rights and ethics, and this is inductive reasoning as I followed a flow from the specific to general.

3- Results:

AI governance is the suitable solution for the human rights and ethics violations resulting from the AI systems installation, because the AI governance will include standards and procedures that prohibit human rights and ethics violations, and in order to reach this stage, the AI governance provides guidelines for AI developers to ensure transparency and accountability during the process of creation and deployment of AI technology.

Also, the cyber governance will include rules which avoid environmental problems as global warming and lack of natural resources. Furthermore, the AI governance prohibits the use of AI sophisticated technology in cyber-attacks and cyber wars, which are major causes of human rights violations.

4-Discussion:

AI governance is a legal framework that includes standards, guidelines and procedures which make the AI systems ethical, safe and respectful to human rights.

AI governance must contain oversight mechanisms that code risks such as bias, privacy violations and mismanagement, and at the same time, AI governance must encourage innovation. Besides, the AI governance must be created by the public and the private sectors, with the help of ethicists and Human Rights Watch to ensure that the development of AI systems is aligned with human rights and society’s value, also there are essential principles in AI governance that cannot be crossed such as transparency, bias control and accountability.

First, transparency is required during the formation of AI systems, and the developers of AI must ensure clarity and openness in how the AI systems function and take decisions.

Second, to avoid bias, the developers must be very accurate in training the AI systems. For instance, the programmer must be accurate in the data entry process because any incomplete or malicious data entering will cause a dangerous problem. For example, we should not enter the option of ethnicity or gender while designing an AI system for hiring new employees to avoid discrimination.

Third, accountability means that AI developers must show responsibility for their wrong actions during the development and deployment of AI systems, which means that the programmers of AI tech must admit their errors like bad deployment. For example, installing an AI system which was developed for schools with special needs in normal schools.

Moreover, the AI governance must provide the AI systems users with technical guidelines to evade safety and ethical problems and the steps of these guidelines are as the following:

1.Direct observation of AI systems: the AI systems must be presented on a dashboard of the AI companies that gives updated information about the status of the AI systems.

2.Self-monitoring: AI systems should have automated detection systems for unethical performance and there must be performance alerts in case the AI model diverges from its preset performance restrictions.

3.Deployment of evaluation metrics: it is an essential and vital point of AI system quality. Normally the metrics are procedures used to evaluate the performance of the machine model.

Furthermore, AI governance must be the protector of the environment, and we mentioned previously that there are many environmental problems caused by AI tech deployment, such as global warming and scarcity of natural resources.

The AI data center consumes a lot of electricity, which increases greenhouse emissions, and that causes global warming globally. For that reason, the AI governors must oblige the giant tech companies to reduce their consumption of electricity and try to find another source of energy which is friendly to the environment, like the solar energy system. Also, the giant tech companies must invent AI models that do not require a lot of energy consumption. For instance, the CHATGPT model consumes a lot of energy, but there is a similar version of CHATGPT called the Deepseek which can use up to 40 times less energy than the CHATGPT, and this kind of AI application with less energy consumption is the ideal model for the AI governance standards.

Additionally, AI governors must forbid the overconsumption of natural resources such as water and lithium, and there must be a maximum level of quantity consumption per year for those

Resources which cannot be exceeded by the AI companies in order to avoid the scarcity problem. Besides, the illegal use of AI technology in cyber-attacks is forbidden in cyber governance because it leads to human rights violations. Also, armies must be ethical in using AI technology during their warfare, since the AI technology performs on the battlefield according to the commander's guidance, so the commander must ensure that the guidance doesn't violate human rights by killing or harming civilians.

As we can see from the previous examples in research that there is a negative relationship between the deployment of AI systems and the unemployment rate, and to prevent this problem, the AI government must have a compensation plan for employees who are going to be replaced by AI models. Also, there must be a rule in cyber governance which obliges employers to create new job opportunities aligned with the implementation of AI systems, because studies prove that there will be new kinds of jobs for people in the future as a result of AI systems installation in the work environment. Besides, AI governance must prohibit the theft of intellectual property.

5- Conclusion:

AI governance is a legal framework that contains policy, procedures and guidelines which should be implemented to avoid problems like the high unemployment rate resulting from the extensive deployment of AI systems in jobs, and there must be a rule that forces employers to pay compensation to the people who were replaced by the AI systems. Also, AI companies must provide people with new job opportunities accordingly with the AI installation in the work process.

Moreover, the AI governance prohibits the excessive consumption of natural resources such as water and lithium. Besides, AI governance obliges the giant tech companies to find a new source of energy for their AI data centers, like solar energy. Also, AI governance illegalizes the use of sophisticated AI systems in cyber-attacks, and armies should always respect ethics and human rights during the use of AI systems in their wars.

Furthermore, the AI governance must always avoid any AI action which leads to human rights violations as like privacy, discrimination and data protection. Besides, the developers of AI models should always take into consideration transparency, bias control and accountability while building and implementing AI systems.

Our research is similar to an article named Artificial Intelligence and Human Rights which declared that the AI has negative impacts on human rights:" Rapid adoption of AI technologies has led to rising concern about potential negative implications for human dignity." (Metzger, 2019) Besides the authors of this article suggested using human rights as the framework of cyber governance which is similar to our suggestion in the discussion, but the articles were limited to human rights, and it did not propose a detailed solution for this problem.

On the other hand, there are many opinions which contradict the idea of AI governance for many reasons.

First, the AI products deployment and the AI research fields are now in the hands of the private sector and those duties used to be for the public sector, and generally the private sector does not encourage the idea of AI governance:" the tragedy of AI governance is that those with the greatest leverage to regulate AI have the least interest in doing so, while those with the greatest interest have the least leverage." (Chesterman, n.d.)

Second, most states are afraid that AI regulations could be too aggressive and could negatively affect AI innovations.

Furthermore, AI governance is facing many challenges such as:

1. The rapid growth of technology: the AI is in continuous development, which considers problems for the legislators of AI governance, since this unstoppable development may create new human rights violations and ethical problems which are not covered in the existing AI governance.

2. Regulation confusion: most of the laws in AI regulations are taken or interfere with other existing domestic regulations. This can create confusion in the legal framework of AI governance, because AI governance is based on international laws and the use of existing national laws by governors will be a problem due to the differences between the two kinds of laws.

3. The large number of actors in AI governance: there are many participants in AI governance as public sector, private sector and social committees, which may lead to decision-making problems, as participants may have different opinions and this could create a conflict of interest between them, which can be problematic for the decision-making process.

Furthermore, the point of strength of this research is classifying a variety of new rules and laws under one AI governance that can help to solve many problems and this will empower more the AI governance globally. For example, we mentioned the environmental problems caused by the AI technology such as global warming and natural resources scarcity, and normally those problems are related to other environment regulations, but putting them under AI governance is a new idea, and it will help to solve the global warming problem, besides suggesting a compensation plan for the unemployed people and obliging the giant tech companies to offer new job opportunities are essential to solve a big futuristic problem, also prohibiting the use of AI technology in cyber-attacks will help in diminishing the losses in cyberspace.

On the opposite hand, the point of weakness in the research is that the AI systems could make unpredictable actions by inputting too much information inside the AI systems and by giving them more authority in decision-making, and this could lead us to more human rights violations which are not covered in the suggested AI governance of this research.

References

(n.d.). Retrieved from https://w.media/australian-governments-review-into-ai-focuses-on-data-centre-sustainability/

Aljazeera . (n.d.). Retrieved February 12, 2025, from https://www.aljazeera.com/news/2025/2/12/paris-ai-summit-why-wont-us-uk-sign-global-artificial-intelligence-pact

Bashkaran, G. (n.d.). *CSIS*. Retrieved November 29, 2023, from https://www.csis.org/analysis/why-responsible-mining-human-rights-imperative

Belenguer, L. (2022). AI Bias: Exploring Discriminatory Algorithmic Decision-Making Models andthe Application of Possible Machine- Centric Solutions Adapted from the Pharmaceutical Industry. *AI and ethics* , 771.

Borgesius, F. J. (2020). Strengthening Legal Protection Against Discrimination by Algorithms and Artifcial Intelligence'. *International Journal of Human rights* , 15-72.

Chen, S. (n.d.). Retrieved April 10, 2025, from https://www.scientificamerican.com/article/ai-will-drive-doubling-of-data-center-energy-demand-by-2030/

Chesterman, S. (n.d.). Retrieved October 2023, from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://law.nus.edu.sg/wp-content/uploads/2024/01/027_SimonChesterman.pdf

Council of Europe . (n.d.). Retrieved May 17, 2024, from https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence

Crawford, M. A. (2018). Seeing Without Knowing: Limitations of the Transparency Ideal and its Application to Algorithmic Accountability' . *New Media and Society* , 973-89.

D'andrea, A. (n.d.). *Keeper* . Retrieved December 13, 2024, from https://www.keepersecurity.com/blog/2024/09/13/how-ai-is-making-phishing-attacks-more-dangerous/

Delman, M. (n.d.). Retrieved from https://www.soterosoft.com/blog/ai-powered-ransomware-the-next-generation-of-damaging-cyberattacks/

Dhanabalan Thangam& M, H. R. (n.d.). Retrieved March 2024, from https://www.researchgate.net/publication/378597789_Impact_of_Data_Centers_on_Power_Consumption_Climate_Change_and_Sustainability

Eliott, D. (n.d.). *World Economic Forum*. Retrieved February 04, 2025, from https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

European Parliament . (n.d.). Retrieved June 8, 2023, from https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#:~:text=In%20April%202021%2C%20the%20European,risk%20they%20pose%20to%20users.

Falcon, S. (n.d.). *Nurse.org*. Retrieved March 1, 2024, from https://nurse.org/articles/nurse-robots/

Feldstein, S. (n.d.). *Carnegie Endowment for International Peace*. Retrieved December 17, 2019, from https://carnegieendowment.org/2019/09/17/global-expansion-of-aisurveillance-pub-79847

Ferguson, A. (2021). Facial Recognition and the Fourth Amendment . *Minnesota Law Review*, 1105-1107.

Global AI governance . (n.d.). Retrieved from https://globalaigov.org/tools/treaties/

Gordon, C. (n.d.). Retrieved February 25, 2024, from https://www.forbes.com/sites/cindygordon/2024/02/25/ai-is-accelerating-the-loss-of-our-scarcest-natural-resource-water/

Gross, J. F. (n.d.). *NBER*. Retrieved from https://www.nber.org/papers/w28061

Jacque, L. (2021). Facial Recognition Technology and Privacy: Race and Gender-How to Ensure the Right to Privacy is Protected' . *San Diego International Journal* , 111-135.

Jones, L. (2020). A Philosophical Analysis of AI and Racism' . *Stance*, 36-41.

Joshi, D. (n.d.). Retrieved February 24, 2025, from https://odi.org/en/insights/the-paris-ai-summit-is-geopolitical-rivalry-derailing-ai-governance/

Kafeero, S. (n.d.). *Quartz Africa* . Retrieved December 27, 2020, from https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters

Koops, B. J. (n.d.). The Concept of Function Creep'. *Innovation and Technology* , 29-53.

Laws. (n.d.). Retrieved January 25, 2025, from https://lawvs.com/articles/ipr-and-human-rights#:~:text=The%20various%20kinds%20of%20IPR,literary%2C%20or%20artistic%20production%E2%80%9D.

Mauzur, P. (n.d.). *The New York Times* . Retrieved April 14, 2019, from https://www.nytimes.com/2019/04/14/technology/china-surveillance-artifcial-intelligence-racial-profling.html>.

Metz, C. (n.d.). *The New York Times* . Retrieved March 15, 2021, from https://www.nytimes.com/2021/03/15/technology/artifcial-intelligence-google-bias.html>.

Metzger, E. D. (2019). Artificial Intelligence and Human Rights . *Journal of Democracy*, 115-126.

Millet, T. (n.d.). *Colombia Journal of Transnational Law Bulletin* . Retrieved October 18, 2020, from https://www.jtl.columbia.edu/bulletinblog/a-face-in-the-crowd-facial-recognition-technology-and-the-value-of-anonymity

Prowriters . (n.d.). Retrieved from https://prowritersins.com/cyber-insurance-blog/legal-issues-involving-artifical-intelligence/

Rawashdeh, S. (n.d.). *University of Michigan-Dearborn*. Retrieved March 2023, 2023, from https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained

Ridhhi Setti. (n.d.). Retrieved February 06, 2023, from https://news.bloomberglaw.com/ip-law/getty-images-sues-stability-ai-over-art-generator-ip-violations

Schenieder, B. (n.d.). *University Of Oxford*. Retrieved May 05, 2023, from https://www.economics.ox.ac.uk/publication/1339882/ora-hyrax

Schmitt, M. N. (2013). *Tallinn Manual on the international law applicable to cyber warfare.* Cambridge University Press.

Science and Technology . (n.d.). Retrieved February 14, 2025, from https://www.drishtiias.com/daily-updates/daily-news-analysis/paris-ai-summit-2025#:~:text=Key%20Themes%20of%20Paris%20AI%20Action%20Summit%202025%3A&text=Innovation%20%26%20Culture%3A%20Creating%20sustainable%20AI,effective%20international%20AI%20governan

Shwarz, E. (n.d.). Retrieved from https://www.qmul.ac.uk/research/featured-research/the-ethical-implications-of-ai-in-warfare/

singh, T. s. (n.d.). Retrieved October 18, 2021, from https://www.iea.org/commentaries/what-the-data-centre-and-ai-boom-could-mean-for-the-energy-sector

Sloan, K. (n.d.). *Reuters* . Retrieved August 13, 2021, from https://www.reuters.com/legal/legalindustry/calif-bar-attorneys-disable-alexa-when-work

UN News . (n.d.). Retrieved December 30, 2020, from https://news.un.org/en/story/2020/12/1080192

UNESCO. (n.d.). Retrieved from https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

Vidgor, N. (n.d.). *The New york Times* . Retrieved December 15, 2019, from https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html

Wan, L. W. (2025). The Impacts of Robots on Unemployment duration: Evidence from the Chinese General Society Survey. *China Economic Review* .

Wexler, R. (2018). Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System. *Stanford Law Review*, 13-49.

You, J. (n.d.). *EPOCH*. Retrieved February 07, 2025, from https://epoch.ai/gradient-updates/how-much-energy-does-chatgpt-use

"دور الذكاء الاصطناعي في انتهاكات حقوق الإنسان وأهمية إدارة الذكاء الاصطناعي في حماية حقوق الإنسان"

إعداد الباحث:

د. زياد زهيري

الملخص:

أنظمة الذكاء الاصطناعي هي تكنولوجيا جديدة تغير حياتنا، لأنه في الوقت نفسه، يمكننا إيجاد الذكاء الاصطناعي في كل شيء. على سبيل المثال، توجد تكنولوجيا الذكاء الاصطناعي في هواتفنا، منازلنا، سياراتنا، أعمالنا، حواسيبنا، مستشفياتنا وأماكن أخرى، وهذه قضية حاسمة، حيث أن تكنولوجيا الذكاء الاصطناعي سلاح ذو حدين وهناك جانب جيد وآخر سيء في هذه التكنولوجيا، في هذا البحث نركز على الجانب السيء، وبالتحديد الآثار السلبية لتكنولوجيا الذكاء الاصطناعي على حقوق الإنسان والأخلاق. علاوة على ذلك، تعتبر أنظمة الذكاء الاصطناعي تهديداً للخصوصية، وحماية البيانات، والبيئة، ومعدل البطالة، والحروب السيبرانية، وحقوق الملكية الفكرية وغيرها. بالإضافة إلى ذلك، كانت هناك الكثير من المحاولات غير الناجحة من جميع الدول حول العالم لإنشاء تنظيمات لتكنولوجيا الذكاء الاصطناعي، مثل قمة باريس، وقد أدت هذه الفشل إلى اقتراح إدارة الذكاء الاصطناعي كالتنظيم الرسمي لتكنولوجيا الذكاء الاصطناعي. أيضاً في هذا البحث، استخدمنا الطرق المختلطة (الكمية والنوعية) في جمع بياناتنا، وكانت مصادر بياناتنا موثوقة وذات مصداقية بناءً على معاييرنا للمصداقية، كما استخدمنا الاستدلال الاستقرائي في بحثنا.

الكلمات المفتاحية: تكنولوجيا الذكاء الاصطناعي، إدارة الذكاء الاصطناعي، الحرب السيبرانية، البيئة، انتهاكات حقوق الإنسان، الأخلاق.