



## Artificial Intelligence in the era of human rights

Dr. S Krishnan<sup>1</sup>, Pankhuri Sharma<sup>2</sup>

<sup>1</sup> Associate Professor, Seedling School of Law and Governance, Jaipur National University, Jaipur, Rajasthan, India

<sup>2</sup> Seedling School of Law and Governance, Jaipur National University, Jaipur, Rajasthan, India

### Abstract

Artificial Intelligence has the potential to help human beings maximize their time, freedom and happiness. At the same time, it can lead us to a dystopian society. Therefore, finding the right balance between technological development and protection of human rights is an urgent matter on which relies the future of the society we want to live in. "Use of Artificial Intelligence in our life is growing, currently covering a wide range of domains. Something seemingly trivial like avoiding traffic jam by use of an intelligent navigation system or getting the offers directed by a trustworthy trader is the result of data analysis that can be used by AI systems", stated Dunja Mijatović, European Council Commissioner for Human Rights.

**Keywords:** Artificial intelligence, human rights, society, robot laws, robot ethics

### Introduction

Artificial intelligence (AI) is a smart digital system that learns on its own, develops its own search and learning systems, can even have its own language (without being understood by humans), develops its own artificial neural networks, can write its own programs, but most important is the fact that it has decision-making power. Depending on the knowledge it has, it can decide the actions that it does or does not do, being able to predict their result. In other words, AI is no longer dependent on human command. Therefore, AI evolves alone, by analyzing the data, gradually expanding its neural networks, improving its performance. It learns at a higher speed than humans, it plans its way of learning and structuring the data and, above all, decides on its own.

In 1942 the Russian science fiction writer Isaac Asimov conceived the "Three Laws of Robotics": 1) A robot cannot hurt a man or, by inaction, cannot allow a man to be injured 2) A robot must obey the orders given by humans unless such orders would contravene the first rule 3) A robot must protect itself as long as this protection does not contravene the first and second rules.

For 75 years, these clauses have inspired research and cohesion regarding the rights of robots. However, today, Asimov's rules seem rather simplistic and outdated because they focus more on humans than on robots.

The impact of computers on the world since the advent of the first UNIVAC computer in 1946 has been profound. At first, the idea of having a personal computer in the office, home or school seemed inconceivable. Today personal computers are accepted as part of our modern world. Computer processors are used to operate cars, TVs, offices, airplanes and defense systems, and these are just a few examples. The next stage of the progress of computers as mobile units, robots, can, like the personal computer, become a regular partner at home and at work.

The spearhead of computer technology is the development of Artificial Intelligence (AI) and the realization of living computer circuits, called biochips. AI development requires a leap in the computer interface, a huge leap over various data, things that a programmable machine has failed to do. Effectively, the computer must skip the variables, instead of

analyzing them individually. One of the essential difficulties in developing such thinking of computers is the conversion of the holistic thinking process into linear descriptions of written language. The analysis of the common sense is not in line with the FORTRAN programming logic language. "For example, there is no programming language today that makes the difference between a dish and a mug".

During these explosive times of high-tech innovation, the contact between machines with artificial intelligence and humans will grow rapidly. Intelligent computer devices, especially specialized systems, now make decisions in medicine, oil exploration, space exploration, air traffic control, trains and graphic design to name just a few of the impact areas. The most important quality of specialized systems is their infinite ability to store even the most insignificant information and to access it at huge speeds and to compare it with other information in order to make instant decisions.

While it is expedient to briefly conceptualize the 'Artificial Intelligence' as a definition, it is to be noted that there is yet to be an agreed-upon concept. Many definitions of A.I. have been offered, the first of which came in 1956 during the Dartmouth Summer Research Project on A.I. John McCarthy, one of the founding fathers of the discipline, defined "intelligent" any system capable of performing actions that would be qualified as intelligent if a human being accomplished them. By this definition, artificial intelligence is simply a machine or a system that is capable of performing any task a human being can perform. A recent Stanford University report defines AI as "a science and a set of computational technologies that are inspired by—but typically operate quite differently from—the ways people use their nervous systems and bodies to sense, learn, reason, and take action." 4 In another definition, Stuart Russell and Peter Norving suggest that AI can be broken down into the following categories: 1) systems that think like humans; 2) systems that act like humans; 3) systems that think rationally; and 4) systems that act rationally. 5 All these established definitions are channeled to the sole fact that Artificial Intelligent systems are designed to ease the workings of humans.

## The Impact of AI in Society

AI is no longer a fiction or a laboratory research, it is a reality that has begun to have a major impact on society. For this impact we must prepare. What an AI can do is pretty much everything a person can do at work. It can handle objects, it can recognize handwriting, it can recognize faces with great accuracy - it can even recognize the emotional state of the human being after the features of the face at that time - it can understand the language and even translate instantly when appropriate, it recognizes fingerprints and can detect obstacles, weather forecasts, medical diagnoses and has the ability to adapt quickly, without problems, under extreme conditions, etc.

Randall Davis of MIT says about artificial intelligence the following: 1) it can solve problems 2) it can explain results 3) it can learn from experience 4) it can structure its knowledge 5) it is able to break rules when necessary 6) it can determine relevance. Currently, computers are capable of accomplishing the first three tasks, but they cannot be reprogrammed alone, nor can they break rules.

An essential thing that should be considered is the privacy, the protection of personal data in the interaction with an AI. Personal data are information relating to the person, that is, that information concerning the personal, public or professional life - information regarding the physical or physiological identity, physical or digital address, information posted on websites, medical information, information related to digital codes of accession.

The collection and / or processing of personal data means any operation that is carried out on personal data, which one does. This data can be collected by an AI which is able to find out the most intimate things about a person in a very short time. From blood pressure, blood composition and the diseases they suffer from, to physical or digital addresses, where that person was, with whom and what he/she talked about that day, or what his/her bank accounts are.

In the context of the above, this question is also essential: what freedoms and rights will we have in the "AI era"? How far will be the right to privacy respected?

On the occasion of the Davos meeting in January 2018, at the World Economic Forum, the ability to adapt companies to the new and revolutionary AI challenge was discussed. What has been made very clear was that "the fourth industrial revolution will eliminate millions of jobs". Another essential aspect that has been specified and must be kept in mind is that we need a concomitant revolution in training and education, encouraging innovation and adaptability.

As you can see, AI can do - and even with much higher efficiency (- everything that man does at present, at work. Will entrepreneurs prefer to implement AI in their companies or will they prefer human staff? There are companies that have already purchased and developed AI. So, we think the answer is predictable: yes, companies will prefer AI because the costs are much lower, and the efficiency increases considerably. AI does not get tired, does not need a meal break, does not need rest and does not have to work only 8 hours a day; moreover, it does not need a salary. If we look at what an AI can do in relation to human capacity, then it is even more effective and it can be considered superior. Will it be so? If so, how will society approach such a situation, such a change?

Society has to learn much more quickly to adapt to the new, otherwise personal misunderstandings and tensions will give

rise to conflicts that can lead to wars. It is necessary to realize that it is a responsibility on our part to educate the new generations, considering the future from this perspective. Everything is based on education and lifelong learning, respect for moral principles and especially respect for everything around us.

## Conceptualizing Human Rights Under Relevant Domestic and International Laws

The concept of human rights has been treated with intense attention and as a delicate issue as it covers the very existence of every person, irrespective of geographical and cultural differences. Human Rights are the basic entitlements of all human beings in any society. They pertain to humans by virtue of their humanity. They are the irreducible minimum requirement for a civilized human existence in any society. As a concept, human rights can broadly be defined as the basic rights of human beings that is centered on equality, fairness, freedom, and respect for all. Human rights were succinctly defined by Kayode Eso J.S.C (as he then was) in the case of *Ransome Kuti & ORS v. A.G Federation & ORS* as thus: "[Human rights] are rights that have always existed, even before orderliness prescribed rules for the manner they are to be sought. It is a primary condition to a civilized existence which stands above the ordinary laws of the land."

Human rights are the freedoms, liberty, immunities or benefits which according to natural law, modern values and international law, all human beings are entitled to enjoy as a matter of right in the country or society in which they live. Human rights are very fundamental to every human that persons cannot live without them, Human rights are what enables a person to continue his humanity. Without human rights, life is meaningless, worthless and a mere shadow. To wit, human rights are too precious to be infringed upon without sufficient and convincing justification.

Although there is the provision of human rights in the laws of many countries, there is notably an international provision of same. In actual fact, the existence and recognition of human rights internationally is antecedent to many of the entrenchment of human rights in many countries. To this end, there are international laws made by international bodies that equally focus on human right as a subject matter; these laws are subject to the ratification and enactment of the member countries.

One of the most important international laws that treat human right is the Universal Declaration of Human Rights, 1948. "Universal Declaration of Human Rights" (UDHR) is one of the important documents that declared fundamental rights for human and requested all of the states to protect these rights. The UDHR law is very fundamental to the history for law; it is a response to the yearn for the inclusion of human rights as an internationally recognized law. Drafted by representatives with different legal and cultural backgrounds from all regions of the world, the Declaration was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 as a common standard of achievements for all peoples and all nations. It sets out, for the first time, fundamental human rights to be universally protected.

Another international law that spells out a category of human rights is the International Covenant on Civil & Political Rights. The International Covenant on Civil and Political Rights (ICCPR) has its foundation in the Universal

Declaration of Human Rights. The rights guaranteed by this covenant are the basic rights which are generally enforceable by instituting a judicial action in the legal system of democratic countries.

### **The Impacts of Artificial Intelligence on Relevant Human Rights**

Human rights, defined to be a necessity to the living of any human, has been questioned on its stance with the development of Artificial Intelligence. The developments have generated opinions on its necessity and its avoidance. One important thing must be noted which is that humans themselves create artificial intelligent systems. On this reason, humans have developed AI due to the activities of man and its help in making these activities easier and faster. AI is not being developed in a vacuum or deployed against a blank slate. Rather, specific actors in society are deploying AI to automate decision making in particular fields of endeavor. They are doing so to achieve outcomes that they view as desirable, against the backdrop of social institutions that have their own, preexisting human rights implications. Elementally, the designed structure of Artificial Intelligence taking decisions for man has generated many positions as to its influence of human rights. These positions are either positive or negative.

Indubitably, aligning with the prospect of Artificial Intelligence, it evinces its contribution to the easement of every arm of life. In the creation of certain intelligent systems, the monitoring of human rights abuses has become easier; and consequently, the proof of human rights violation has become less rigorous in courtrooms. Digital technology in the twenty-first century has ushered in what some have called the "golden age of surveillance"—not only by states and corporations but also by non-state actors. Human rights groups, news organizations, and open-source investigators such as Bellingcat and the Syrian Archive access massive amounts of open-source data generated by billions of sensor platforms in the hands and pockets of people around the globe.

With the proliferation of multipurpose mobile phones and other imaging platforms, including hundreds of high-resolution imaging satellites, something approaching ubiquitous surveillance has emerged. By this, it is almost impossible for any activity or occurrence to not be recorded by a camera, either on the ground or in orbit. This wave can be denoted in two ways; positively and negatively. In the positive aspect, the security of a state can be improved via the use of artificial intelligence. This includes the fight against terrorism. In 2017, for instance, the International Criminal Court issued an indictment for the arrest of a Libyan warlord based on satellite imagery and videos taken of the executions he ordered (or conducted himself) and that were posted to social media by his followers. This and many more is the advantageous side of Artificial Intelligence in human rights.

### **Artificial Intelligence, new risks for human rights**

AI has proven the latest 'weapon' to be employed by states and other actors, increasing both current and new risks to national and global security. AI offers the possibility to analyze human behaviors, moods, and beliefs based on available data. Malicious use of AI exacerbates risk, increasing its negative impact, including its influence on maintaining or disrupting democratic balances. The right to

life, freedom, privacy, and universal values and principals are threatened by AI.

### **Right to life threatened by autonomous weapons systems**

The right to life is central in the debates surrounding the potential impact of AI and autonomous weapon systems. As stated in the *Preamble to the Charter of United Nations*, "We the people of the United Nations are determined to save succeeding generations from the scourge of war" (United Nation) and the Universal Declaration of Human Rights (UDHR) recognizes in Article 3 that "Everyone has the right to life, liberty, and security of person." But the growing investment in lethal autonomous weapons is a serious threat to this right. Worldwide spending on robotics is expected to reach \$87 Billion by 2025.

International law aims to ensure peace and security, but AI has imposed new challenges that limit its efficiency. These challenges have been increased by the COVID-19 pandemic, which is facilitating the transition to a new world order different from the global order established after the Second World War.

In the same context, the introduction of autonomous weapons systems (AWS) has created a controversial discussion between states because they are real risks to the right to life, which requires an urgent review of the use of force, as cited in the UN Charter. According to Burri "fully autonomous weapons systems (i.e., systems that select and engage targets without meaningful human control) are likely to be banned through a new international legal instrument, while the use of weapons systems equipped with a low level of autonomy will be lawful". Goldstein argued that state competition toward AWS leads us to the assessment that the current trade crisis between China and the US may be escalated to an open military conflict with the use of AI weapons. Fully AWS, or as they have been called by the (Human Rights Watch), "human-out-of-the-loop weapons", are currently the most dangerous threat to the right to life, peace, and security. The threat of AWS is "the problem of reaction time, which threatens to turn humans in and on the loop into liabilities". Anderson and Waxman explain that "such systems are much easier to create than lawful ones (Anderson and Waxman). The speed necessary to respond to such adversary systems in the field, though, might well create demand for defensive systems that feature greater autonomy in decision-making" (Anderson & Waxman 8). First, the future of humanity will not be decided by state actors when AWS is employed. Second, all these new technologies are growing faster than international law as stated by (Anderson and Waxman 8). Thus, international norms such as those concerning the use of force and defense need to be revised to ensure peace and security and protect the right to life.

The legitimacy of new weapons is a culminating point in the controversial discussion about AWS. Article 36 of the 1977 revision of the Geneva Conventions provides that "in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this protocol or by any other rule of international law applicable to the High Contracting Party" (United Nations 258). Davison confirms that the commander (human or otherwise) in the use of weapon systems should respect their core legal obligation (3).

Anderson and Waxman also query whether "robots [can] ensure the distinction between military and civilian objects or between active combatants and innocent civilians?" (8). This means that states need to invest more in ethics in artificial intelligence to prevent violations of international humanitarian law. Ethics is the only way to minimize the risks imposed using AI in the military. Thus, states need to collaborate with all stakeholders to ensure the technical and legal protection of human rights in peace and during the war. Rethinking international law and national legislation is now an obligation rather than a choice. In the same context, states need to adapt their policies and international mechanisms alongside evolutions in AWS. They should also review their responsibilities in consideration of the right to life as a significant right threatened by AWS, including during armed conflicts.

### Freedom and Artificial Intelligence

According to Article 19 of the *Universal Declaration of Human Rights* "Everyone has the right to freedom of opinion and expression, this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers" (UDHR). The key question is how can we ensure freedom of expression when public opinion is influenced by AI? This new tool is imposing new risks to freedom.

AI offers new tools to create content (audio and visual analyses) and while the possibility exists for AI to support the freedom of expression, which is a cornerstone for democracy and the enemy for corruption, in reality it increases the control of social media platforms and freedom of expression by the government. AI systems contained in social media are also used to influence public opinion and to guide social movements considering workflow optimization, automated content creation, content creation from legacy archives, content selection for targeting audience demographics, optimization of asset selection, metadata creation, and content personalization (ITU). AI can personalize, generate, and filter content. It has terrifying implications for freedom of expression, social movement, and election campaigns. Questions arise concerning non-trusted or fake information published by the media, but which is selected and kept trending by AI. How can we determine the level of trust in media which can be manipulated by governments, advertisers, algorithms or other third parties seeking to persuade users and recipients of such information?

Some AI systems are more efficient than humans in certain tasks such as mimicking others' voices and images to influence people and to create political changes (also known as deep fakes). There is also the concept of machine learning software that creates fake videos (Cole, 2018) <sup>[8]</sup>. This new technology developed by Chinese tech giant Baidu can reproduce a believable fake voice with just 3.7 seconds of audio much as the concept of machine learning software that creates fake videos (Cole, 2018) <sup>[8]</sup>. In the same context, Montreal-based AI start-up Lyrebird claims it can do text-to-speech using just one minute of audio (Cole, 2018) <sup>[8]</sup>. This means that individuals are no longer in control of the creation and security of their public opinion, rather they are represented by AI. They can no longer trust their own autonomy when their expression of thought is influenced by the information spreading on social networks and their

personal interactions with algorithms are manipulated and abused.

The use of smartphones becomes a real risk to freedom of expression considering the number of arrests in some countries after individuals posted on Facebook calls for freedom during quarantine, such as the Australian woman Zoe Buhler, who was arrested at her home after she created a "Freedom Day" event on Facebook calling for people to protest against the Victorian government's coronavirus lockdown measures (The Guardian).

In Tunisia, Amna Al-Sharqi was arrested for posting a text on her Facebook page entitled "Surah Corona" (The New Arab). According to Freedom House, "Rather than protecting users, the application of national sovereignty to cyberspace has given authorities free rein to crack down on human rights" (Shabaz & Funk 2). A large number of countries are using COVID-19 to justify their engagement in mass surveillance in partnership with companies and telecommunication providers, the most draconian approach being adopted by China (Shabaz & Funk 2).

The pandemic, and the laws adopted by some governments to face disinformation, has created a serious restriction on freedom and privacy and it creates new legal challenges related to international human rights. For that reason, UNESCO has issued guidelines for judges and courts, both at national and regional levels that can serve as references to apply the theoretical frameworks of international law and human rights standards to protect and promote freedom of expression" (UNESCO a).

### Protecting Privacy in The Age of Artificial Intelligence

According to Article 12 of the *Universal Declaration of Human Rights*, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation." However, systems that combine data from satellite imagery, facial recognition-powered cameras, and cell phone location information, etc., can provide a detailed picture of an individual's movements as well as predict future movements and location. It could therefore easily be used by governments to facilitate more precise restriction of the freedom of movement at both the individual and group level and by foreign actors who are targeting political changes (Access Now 21). Voting behaviour and election campaigns are also influenced by social media (Brundage *et al* 29). We are constantly connected to our smartphones which facilitates the search for each case of Covid-19 to mitigate the impact and magnitude of this pandemic. Today's smartphones even allow remote access to a person's electro-gram. This creates new risks and challenges ranging from privacy to freedom of expression, given the tension between individuals and governments regarding human rights and democracy. Facial recognition is one of the programs which raises privacy issues which can increase digital dictatorship. Conversely, "the facial recognition market is expected to grow to US\$7.7 billion in 2022 from US\$4 billion in 2017. That is because facial recognition has all kinds of commercial applications. It can be used for everything from surveillance to marketing" (Symanovich). COVID-19 and AI are taking societies around the world to another phase in history with the increased use of robots for online shopping and deliveries, digital and contactless payments, remote work, distance learning, etc. AI is changing our lives and is influencing all sectors, as argued by the (OECD a).

In this context, digital technology can play a role in contact tracing programs implemented in the Member States. Several countries are using artificial intelligence to ensure access to information and to trace COVID-19 but these apps are also tracking individuals according to Freedom House (Shabaz & Funk 2). Member States are obliged under the International Health Regulations, to develop public health surveillance systems that capture critical data for their COVID-19 response, while ensuring that such systems are transparent, responsive to the concerns of communities, and do not impose unnecessary burdens, for example, infringements on privacy" (WHO 1). This is creating serious tension between states. AI creates new challenges for international law regarding human rights, and it can be a risk to freedom and privacy. According to the World Health Organization, "such uses of data may also threaten fundamental human rights and liberties during and after the COVID-19 pandemic. Surveillance can quickly traverse the blurred line between disease surveillance and population surveillance" (WHO 1). Free and open scientific data impose other challenges that necessitate rethinking international law in consideration of the appearance of new notions linked to the states and their sovereignty.

Open access to scientific data is creating new risks to data sovereignty, which is one of the causes of the conflicts between China and the US. Donald Trump and his administration have accused China of failing to share its samples of COVID-19 with other countries (Riley-Smith). The cause of this conflict is data sovereignty, which is essential to technological sovereignty. In the age of AI, data sovereignty is a *sine qua non* condition of sovereignty.

### Relevant Constitutional Provisions

Artificial intelligence (AI) is posing serious constitutional and human rights issues as it is incorporated into more and more fields, including the workforce. When it comes to the effects of AI on employment, India's Constitution provides a strong framework for defending individual liberties and rights. The main constitutional clauses that deal with AI governance and regulation are listed here, with special attention to those that deal with employment and human rights.

Article 14 of the Indian Constitution guarantees equality before the law and the equal protection of the law to all citizens. AI programs that are used for hiring, managing the workplace, or evaluating employee performance must guarantee equality. It would be against Article 14 for algorithms to support or worsen prejudices based on caste, gender, religion, or handicap. For example, biased training data may cause AI-based recruitment systems to favour specific demographics, which could result in discriminatory hiring practices.

Article 19(1)(a) guarantees the freedom of speech and expression to all citizens. Unrestricted AI technology usage in the employment sector could curb the creativity and innovation of employees and lead to dissatisfaction among both the employees and employers. Further AI technology may be used to track employee's behavioural pattern and may flag unnecessary reports to the employer, further affecting the employees' morale. Article 19(1)(c) guarantees the right to form associations or unions. AI systems that keep tabs on union activity or discourage employees from organising may infringe on their right to organize.

AI surveillance systems that threaten or punish employees for unionising may violate this fundamental right. Article 19(1)(g) guarantees the freedom to practice any profession, or to carry on any occupation, trade, or business. AI can improve career prospects, but if it creates hurdles to work, it also puts this right at danger. One could argue that AI-powered systems that restrict access to particular professions due to prejudicial standards violate people's right to pursue any kind of employment. Furthermore, widespread automation driven by AI may make it harder for workers in some industries to find jobs, which would indirectly affect this right.

Article 21 guarantees the right to life and personal liberty, which has been interpreted by the Supreme Court to include the right to livelihood. The right to privacy was recognized as a fundamental right under Article 21 by the Supreme Court in the landmark case Justice K.S. Puttaswamy (Retd.) v. Union of India (2017). The employment of AI in the workplace, particularly automation technologies that take the place of human labour, may endanger employees' livelihoods. If social security safeguards or other employment alternatives are not implemented, the right to livelihood may be violated by the widespread job displacement brought about by artificial intelligence. This Article may be used to contest laws or procedures that cause widespread AI-related unemployment. AI systems need to respect people's privacy, especially those that are utilised for employee surveillance, data gathering, and profiling. AI solutions used in the workplace for continuous activity monitoring, health data collection, or even facial recognition must respect employees' right to privacy. Without appropriate consent or protections, invasive AI technologies may be contested as violating people's right to privacy.

### Global Legislative Response

The body of law pertaining to AI ethics and privacy is still developing, making it a highly complicated and important topic. AI technologies have the potential to both create privacy issues and provide answers. The General Data Protection Regulation (GDPR) and other privacy regulations are not comprehensive and deep enough to handle the issues raised by AI. Since consent, transparency, and bias prevention are intrinsic problems with AI systems, it may really be the creators of those systems that face these difficulties. The United Nations Educational, Scientific, and Cultural Organisation (UNESCO), the European Council, and the Organisation for Economic Co-operation and Development (OECD) have all established guidelines and recommendations regarding the moral advancement and use of AI. UNESCO has taken a leadership role in addressing the ethical implications of AI.

UNESCO's Recommendations on Ethics of AI, (2021) primary goal is to ensure that AI technologies are developed and used in ways that promote human rights, peace, and sustainable development, while preventing harm and inequity. OECD Principles on AI, (2019) provide detailed guidelines for policymakers to create trustworthy AI systems that support economic growth and societal well-being.

While these organisations have different legal positions, they are all concerned with privacy and transparency (either explicitly or implicitly). The European Parliament passed the EU AI Act 10 in March 2024. Certain AI applications that endanger the rights of citizens are prohibited by the new

regulations. This includes facial recognition databases being created through generic searching of facial photographs from the internet or CCTV footage and biometric categorisation algorithms that rely on sensitive features. Social scoring, predictive policing, and emotion detection in the workplace and classroom are some examples of AI technologies that are prohibited by rules because they have the potential to manipulate people or take advantage of their weaknesses. However, there are no specific, dedicated or exclusive provisions relating to privacy protection.

On October 30, 2023, US President Joe Biden signed an executive order titled "Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI." A "comprehensive approach to AI development and use, focussing on safety, security, privacy, equity, and innovation" is outlined in the directive. There is still no uniform privacy law in the United States, and the Executive Order does not define or clarify what privacy is. The Executive Order lays forth guidelines for upcoming AI policies that will support ethical, transparent, and private AI. Article 22 of the General Data Protection Regulation (GDPR) addresses "Automated individual decision-making, including profiling." The article provides individuals with certain rights when it comes to decisions made solely based on automated processing, which can include profiling. Individuals have the right not to be subjected to decisions based solely on automated processing, including profiling, if those decisions have legal or similarly significant effects on them. In cases where automated decision-making is permitted, there must be suitable measures to protect the data subject's rights, freedoms, and legitimate interests. This includes the right to obtain human intervention, express their point of view, and contest the decision. This is often ignored by various organisations, whereby they have solely relied on AI's automated decisions even in the process of recruitment of employees which has led to several incidents of bias and unreasonableness, prejudicing human rights.

### **The Role of Comprehensive Data Protection Laws**

Comprehensive data protection laws, which should apply to both the government and private sector, can go a long way in addressing many of the human rights risks posed by AI. Because data is the engine of AI, any law that mandates protection of personal data will necessarily implicate AI systems. Given the global push toward data protection legislation, this is both heartening and practical. Consider the impact of the European Union's General Data Protection Regulation (GDPR). The GDPR is a positive framework that provides for control of a person's personal information and empowers people to make informed decisions about how their data are used. The GDPR limits data processing to permissible purposes, with heightened protections for sensitive data. It also requires opt-in consent, which limits the use of personal data for training AI systems. Rights provided for by the GDPR, and other similar laws, offer a framework to prevent against unaccountable uses of AI that impact individual rights, while ensuring a level of control of personal data and accountability for the use of AI and ML systems.

Data protection laws are incompatible with AI and we should make broad exceptions for its development and use. That is misguided. While it is likely true that strong data protection laws may preempt deployment of certain AI systems, companies have never been able to "innovate"

without regard for potential harm. If AI systems are used to make decisions on a basis or rationale that not even their developers can fully explain, at-risk individuals—or AI "guinea pigs"—will be the first to suffer the negative consequences. Data protection rights not only provide accountability structures to mitigate harm, they also protect people against having their personal data covertly co-opted, commodified, and otherwise exploited in ways that harm others or society at large.

The Right to Information and Right to Access work together to allow people to get information about what data an entity is collecting, how they are collecting it, how they will use it, and whether data will be used for automated decision making. These rights raise public awareness about the existence of AI systems and the roles they play. Furthermore, these rights allow people to uncover and understand potential human rights harms and push entities to be more transparent about how they use AI.

The Right to Restrict Processing gives people the ability to request that an entity stop using or limit the use of personal information while the Right to Erasure provides a pathway for deletion of a person's personal data held by a third-party entity when it is no longer necessary, the information has been misused, or the relationship between the user and the entity is terminated. These rights could be used to temporarily halt the use of a contested AI system, or to pressure an entity to use an AI system more responsibly. The Right to an Explanation provides for a person to get an explanation about how an automated decision is made pertaining to that person. This right ensures entities understand how the systems they use actually work, and it pushes AI developers to continue working to make AI understandable. The Right to Object gives people the ability to contest most processing of their personal data by an entity when the data are used for direct marketing, automated decision making (where no human intervention will take place), research and statistics, or for an entity's "legitimate interest." This right allows for direct challenges to decisions made using AI systems. It is particularly important for government use of AI in ways that can be discriminatory. It also ensures there is a human in the loop in important automated decision-making systems, which adds a layer of accountability.

### **Conclusion**

The intersection of artificial intelligence (AI) and human rights within the framework of public international law presents a complex landscape characterized by both challenges and opportunities. As AI technologies continue to advance, it becomes increasingly important to navigate this intersection effectively to protect fundamental rights while leveraging AI's potential to advance human dignity and well-being. This necessitates a multifaceted approach that prioritizes transparency, accountability, and ethical AI practices.

One of the primary challenges in navigating the intersection of AI and human rights is the potential for AI systems to perpetuate biases and discrimination, thereby infringing upon individuals' rights to equality and non-discrimination. AI algorithms, often trained on biased datasets, may produce discriminatory outcomes, particularly in areas such as employment, criminal justice, and access to financial services. Additionally, the opacity of AI decision making processes complicates accountability mechanisms, making it

difficult to attribute responsibility for any resulting human rights violations.

To address these challenges, it is essential to promote transparency and accountability in AI development and deployment. This may involve implementing regulatory frameworks that require AI developers and deployers to document their processes, disclose training data and methodologies, and provide explanations for algorithmic decisions. Furthermore, mechanisms for independent auditing and oversight can help hold stakeholders accountable for the impact of AI systems on human rights.

Despite these challenges, the intersection of AI and human rights also presents significant opportunities for public international law. AI technologies have the potential to enhance access to justice, facilitate the provision of essential services, and promote inclusive decision-making processes. For example, AI-powered tools can improve legal research and analysis, thereby enhancing the efficiency of judicial systems and ensuring fair access to justice for all individuals, regardless of their socio-economic status. Similarly, AI-driven applications in healthcare can support early diagnosis and personalized treatment, contributing to the realization of the right to health.

Moreover, AI can play a crucial role in addressing global challenges such as climate change, poverty, and humanitarian crises. By analysing great ai amounts of data and identifying patterns and trends, AI systems can inform evidence-based policymaking and resource allocation, leading to more effective interventions. Additionally, AI-enabled technologies, such as remote sensing and predictive analytics, can improve disaster response efforts and facilitate humanitarian assistance in crisis situations.

Effectively navigating the intersection of AI and human rights requires collaboration among policymakers, legal practitioners, technologists, and other stakeholders. It is essential to develop and implement regulatory frameworks that promote transparency, accountability, and ethical AI practices while safeguarding fundamental rights. Moreover, ongoing dialogue and engagement with civil society organizations and affected communities are critical to ensuring that AI technologies serve as a catalyst for human rights realization in the 21st century.

## References

1. Abhivardhan. The Wider Realm to Artificial Intelligence in International Law. SSRN, 2018. Retrieved from: [papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3172280](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3172280)
2. Access Now. Human Rights in the Age of Artificial Intelligence, 2018. Retrieved from: [www.accessnow.org/cms/assets/uploads/2018/11/AI-and-HumanRights.pdf](https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-HumanRights.pdf)
3. African Union. African Digital Transformation Strategy, and African Union Communication and Advocacy Strategy among Major AU Initiatives in the Final Declaration of STCCICT3, 2019. Retrieved from: [au.int/en/pressreleases/20191026/african-digital-transformation-strategy-and-african-union-communication-and](https://au.int/en/pressreleases/20191026/african-digital-transformation-strategy-and-african-union-communication-and)
4. AI HLEG. Draft Ethics Guidelines for Trustworthy AI, 2018. Retrieved from: <https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai>
5. Burri T. International Law and Artificial Intelligence. German Yearbook of International Law,2017:60:91–108. Retrieved from:
6. Burri T. International Law and Artificial Intelligence. SSRN, 2017. Retrieved from: <https://ssrn.com/abstract=3060191> or <http://dx.doi.org/10.2139/ssrn.3060191>
7. Brundage M, Avin S, Clark J, Toner H, Eckersley P, Garfinkel B, *et al.* The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, 2018. Retrieved from: <https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf>
8. Cole S. Deep Voice Software Can Clone Anyone's Voice with Just 3.7 Seconds of Audio, using snippets of voices, Baidu's Deep Voice can generate new speech, accents, and tones. Vice Channel, 2018. Retrieved from:
9. Council of Europe. 1353rd meeting, Ad hoc Committee on Artificial Intelligence CAHAI, 2019. Retrieved from: [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectId=09000016809737a1](https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016809737a1)
10. Council of Europe. Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime, 2020. Retrieved from: [https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p\\_auth=2QnPIt18](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=2QnPIt18)
11. Council of Europe. Convention on Cybercrime CETS No.185, 2001. Retrieved from: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
12. Davison N. A legal perspective: Autonomous weapon systems under international humanitarian law, Perspectives on Lethal Autonomous weapon systems. UNODA Occasional Papers,2016:30:5–18. Retrieved from:
13. Davison N. A legal perspective: Autonomous weapon systems under international humanitarian law, Perspectives on Lethal Autonomous weapon systems, 2016. Retrieved from: [https://www.unog.ch/80256EDD006B8954/\(httpAssets\)/6866E44ADB996042C12581D400630B9A/\\$file/op30.pdf](https://www.unog.ch/80256EDD006B8954/(httpAssets)/6866E44ADB996042C12581D400630B9A/$file/op30.pdf)
14. European Commission. Draft Ethics Guidelines for Trustworthy AI, 2018. Retrieved from: [ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai](https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai)
15. European Parliament. Charter of Fundamental Rights of the European Union 2000/C 364/01. Official Journal of the European Communities,2000:C364:1–22. Retrieved from: [www.europarl.europa.eu/charter/pdf/text\\_en.pdf](https://www.europarl.europa.eu/charter/pdf/text_en.pdf)
16. European Union. Consolidation version of the Treaty on European Union. Official Journal of the European Union,2017:C326:17–390. Retrieved from: [https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC\\_1&format=PDF](https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF)
17. Goldstein A. First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations. International Security,2013:37(4):49–89. Retrieved from: [https://www.mitpressjournals.org/doi/abs/10.1162/ISEC\\_a\\_00114](https://www.mitpressjournals.org/doi/abs/10.1162/ISEC_a_00114)
18. Greenberg A. Hackers remotely kill a Jeep on the highway-with me in it. Wired,2015. Retrieved from:

- <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>
19. G7. Charlevoix Common Vision for the Future of Artificial Intelligence, 2018. Retrieved from: <http://www.g7.utoronto.ca/summit/2018charlevoix/ai-commitment.html>
  20. G20 Insights. G20 AI Principles, 2010. Retrieved from: <https://www.g20-insights.org/wp-content/uploads/2019/07/G20-Japan-AI-Principles.pdf>
  21. Human Rights Watch. Losing Humanity: The Case Against Killer Robots, 2012. Retrieved from: <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>
  22. Internet Rights and Principles Coalition. The Charter of Human Rights and Principles for the Internet, 2019. Retrieved from: [https://internetrightsandprinciples.org/wp-content/uploads/2020/03/IRP\\_booklet\\_Eng\\_7ed\\_Nov2019.pdf](https://internetrightsandprinciples.org/wp-content/uploads/2020/03/IRP_booklet_Eng_7ed_Nov2019.pdf)
  23. Leys N. Autonomous weapon systems, and international crises. *Strategic Studies Quarterly*, 2018;12(1):48–73. Retrieved from: [https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12\\_Issue-1/Leys.pdf](https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-12_Issue-1/Leys.pdf)
  24. Waxman M, Anderson K. Law and ethics for autonomous weapon systems: Why a ban won't work and how the laws of war can, 2020. Retrieved from: [https://media.hoover.org/sites/default/files/documents/Anderson-Waxman\\_LawAndEthics\\_r2\\_FINAL.pdf](https://media.hoover.org/sites/default/files/documents/Anderson-Waxman_LawAndEthics_r2_FINAL.pdf)
  25. OECD. OECD Policy Responses to Coronavirus COVID-19, Using Artificial Intelligence to Help Combat COVID-19, 2020. Retrieved from: [oecd.org/coronavirus/policy-responses/using-artificial-intelligence-to-help-combat-covid-19-ae4c5c21](https://www.oecd.org/coronavirus/policy-responses/using-artificial-intelligence-to-help-combat-covid-19-ae4c5c21)
  26. OECD. OECD Principles on AI, 2019. Retrieved from: <http://www.oecd.org/going-digital/ai/principles/>
  27. OECD. OECD AI Policy Observatory, 2020. Retrieved from: <https://www.oecd.org/going-digital/ai/about-the-oecd-ai-policy-observatory.pdf>
  28. Pratt GA. Is a Cambrian Explosion Coming for Robotics? *Journal of Economic Perspectives*, 2015;29(3):51–60. Retrieved from: [www.aeaweb.org/articles?id=10.1257/jep.29.3.51](https://www.aeaweb.org/articles?id=10.1257/jep.29.3.51)
  29. Cole S. Deep Voice Software Can Clone Anyone's Voice with Just 3.7 Seconds of Audio. *Vice*, 2018. Retrieved from: [https://www.vice.com/en\\_asia/article/3k799k/deep-voice-software-can-clone-anyones-voice-with-just-37-seconds-of-audio](https://www.vice.com/en_asia/article/3k799k/deep-voice-software-can-clone-anyones-voice-with-just-37-seconds-of-audio)
  30. Shahbaz A, Funk A. The pandemic is fueling digital repression worldwide, 2020. Retrieved from: <https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow>
  31. Smith BR. Trump's top diplomat claims China not sharing Covid-19 sample with world scientists: Mike Pompeo also accuses China of waiting a month before reporting human-to-human spread. *The Telegraph*, 2020. Retrieved from: <https://www.telegraph.co.uk/news/2020/04/22/trumps-top-diplomat-claims-china-not-sharing-covid-19-sample>
  32. Symanovich S. How does facial recognition work, 2019. Retrieved from: <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html>
  33. The New Arab. Tunisia arrests young woman who made up fake Quran verses about coronavirus, 2020. Retrieved from: <http://english.alaraby.co.uk/english/news/2020/5/6/tunisia-a-arrests-young-woman-for-fake-coronavirus-quran-verses>
  34. The Guardian. Victorian Bar criticizes arrest of a pregnant woman for Facebook lockdown protest post as disproportionate, 2020. Retrieved from: <https://www.theguardian.com/australia-news/2020/sep/03/victoria-police-arrested-pregnant-woman-facebook-post-zoe-buhler-australia-warn-lockdown-protesters>
  35. UNESCO. Draft Text for the Recommendation on Ethics of Artificial Intelligence, 2020. Retrieved from: <https://unesdoc.unesco.org/ark:/48223/pf0000373434>
  36. UNESCO. Preliminary study on the technical and legal aspects relating to the desirability of a standard-setting instrument on the ethics of artificial intelligence, 2019. Retrieved from: <https://unesdoc.unesco.org/ark:/48223/pf0000367422>
  37. UNESCO. Protecting Freedom of Expression during the COVID-19 crisis: UNESCO issues Guidelines for Judicial Operators Part 2, 2020. Retrieved from: <https://en.unesco.org/news/protecting-freedom-expression-during-covid-19-crisis-unesco-issues-guidelines-judicial>
  38. United Nations. The Charter of the United Nations, 1945. Retrieved from: <https://www.un.org/en/charter-united-nations/>
  39. United Nations. Universal Declaration of Human Rights General Assembly resolution 217 A, 1948. Retrieved from: <https://www.un.org/en/universal-declaration-human-rights/index.html>
  40. United Nations. Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts Protocol I, 1977. Retrieved from: [https://www.un.org/en/genocideprevention/documents/atrocities-crimes/Doc.34\\_AP-I-EN.pdf](https://www.un.org/en/genocideprevention/documents/atrocities-crimes/Doc.34_AP-I-EN.pdf)
  41. Wolfgang M, Lukic V, Sander A, Martin J, Küpper D. Gaining Robotics Advantage, 2017. Retrieved from: <https://www.bcg.com/publications/2017/strategy-technology-digital-gaining-robotics-advantage>
  42. World Health Organization. Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing, 2020. Retrieved from: [https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics\\_Contact\\_tracing\\_apps-2020.1](https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1)
  43. Yan X, Ziang F. 10 technology trends to watch in the COVID-19 pandemic, 2020. Retrieved from: <https://www.weforum.org/agenda/2020/04/10-technology-trends-coronavirus-covid19-pandemic-robotics-telehealth/>