

KEJSI RIZO

Mediterranean University of Tirana

& Albanian Ombudsman

kejsirizo@gmail.com

ORCID ID: 0000-0002-6436-4925

IMPLICATIONS OF DAILY APPLIED ARTIFICIAL INTELLIGENCE AND THE FUTURE OF OUR RIGHTS

STEPS TOWARDS A LEGAL FRAMEWORK

ABSTRACT

Nowadays, artificial intelligent technologies are all in our hands, and we all make a modest contribution, sometimes consciously and sometimes unconsciously, in their further improvement. The increasing development, adoption and use of intelligent technologies and systems has shown that an algorithm is able to predict consumer's needs, or furthermore wishes, or diagnose a disease with an accuracy rate beyond average natural human intelligence. While the use of artificially intelligent technologies and machines revolutionizes crucial sectors such as health, finance and banking and the economy and market needs, boundaries are still to be set. This paper analyzes ethical implications of day-to-day use of AI along with the need and steps towards human rights law to address AI impacts.

KEYWORDS: *Artificial Intelligence; Human Rights; Face Recognition Technology; Automated decision-making.*

While there is no accepted definition of artificial intelligence (AI), there are many different ways to answer the question what is artificial intelligence? The term "intelligence" refers to the ability to acquire and apply knowledge and skills, while the term "artificial" refers to something made or produced by human beings rather than occurring naturally, especially as a copy of something natural. Therefore, the term artificial intelligence assumes that the

human ability to understand, to comprehend, to sort the important from the unimportant can be replicated by constructing computer programs that are as good or sometimes even better than humans at understanding. AI systems display intelligent behavior by analyzing their environment, with some, degree of autonomy, to achieve specific goals. While artificial intelligence is developing and implementing at a very fast pace, this ratio is inversely proportional when it comes to developing the legal framework at international and national levels. In this sense, for some time now there have been constant attempts to understand and translate the application of these intelligent systems into the language of law.

The need for legal and institutional arrangements of issues arising from the increasingly frequent use of artificial intelligence in all aspects of human daily life, trying to dominate the undesirable effects that may arise from intentional misuse or from ordinary human carelessness, has become absolutely necessary. Wise and timely interventions by legislative institutions give hope that these consequences, if not avoided, at least be reduced and become harmless.

Artificial intelligence is evolving rapidly and its use will spread significantly in the coming decade. Further development of AI creates opportunities for renewal and improvement of healthcare, education or climate change. We are already surrounded by many applications of AI in our computers, phones or in public places. But, there is still one crucial question to answer: are our legal systems well equipped to deal with these innovations? Application of AI is to be examined through the angle of ethics and morality, to monitor its impact or potential risks posed for human rights, antidiscrimination, rule of law and democracy in general. A fundamental rights-centered approach to AI should be underpinned by legal regulation, where the responsibility for protecting rights rests with the state. This should entail (at minimum) the duty to ensure human rights prior to the application of AI-systems. The question is whether existing human rights law can adequately protect against all risks posed by AI systems (including sufficiently justifying a ban of certain AI systems) or whether we need additional human rights or have to adapt certain human rights.

The use of artificial intelligence, particularly the use of *advanced surveillance technology* based on AI, in police enforcement and investigation is a “red area” which gives rise to serious concerns.

Facial recognition technology (FRT) has an inherent risk of discrimination because of lack of human rights-based *design* and *development* (which leads to wrongful data set collection, poor training of the model, lack of testing in relation to biases and discriminatory risks). FRT has been proven to have a larger margin of error for women and people of color. Moreover, central human rights issues rise in relation to its *application*: FRT captures biometric data which is highly sensitive and thus subject to strict necessity test. FRT used for mass surveillance is especially highly problematic both because of privacy concerns and because of risk of chilling effect on freedom of assembly and expression. On the other hand there is a lack of common European rules and safeguards for police use of FRT which is being tested across Europe, and lack of rules that ensure human rights by design and human rights impact assessment (HRIA) prior to the application of FRT and – drawing on established good practice from other fields – repeated on a regular basis post application. More generally, there is a lack of clear regulatory safeguards in the cooperation between States and developers of surveillance technology, therefore explicit human rights safeguards in e.g. public procurements of surveillance technology by police and intelligence services, are needed.

Automated decision-making (ADM) based on algorithmic profiling gives rise to serious human rights concerns (both in relation to the private sector and the public administration). The lack of transparency in the design and development of algorithmic profiling based on machine learning leads to the so-called “black box”-problem¹. This creates challenges in relation to data protection (access to information) and discrimination in particular. Without transparency, wrongful (or discriminatory) use of personal data (including protected characteristics) cannot be identified by neither the developer, the public or private entity making use of ADM or the individual whose rights are potentially violated. In this regard there is a lack of set of rules that ensure transparency in the design and/or a comprehensive right to explanation of the algorithmic model in the application of ADM by public and private entities, and lack of rules that ensure human rights by design and human rights impact assessment prior to the application of an AI-system and – drawing on established good practice from other fields,

¹ The Black Box Problem is any artificial intelligence system whose inputs and operations are not visible to the user or another interested party.

and repeated on a regular basis post application. One should not forget that similar system of ADM is used as “robot judge”².

A human rights impact assessment on AI should consider the potential impact on the full range of rights, and not be limited to data protection, privacy and non-discrimination which have up until now been a main focus. Also, it should be avoided that the lack of access to internet, along with digital illiteracy, in the context of a true ‘digital revolution’ enhances fundamental rights violations impacted disproportionately on certain vulnerable groups. Main elements of a legal framework should include clarity on situations in which the framework applies; human rights impact assessment prior to procurement, design, development and application as well as regular assessment during deployment; transparency and information on purpose, policies, inputs and outputs of an AI system so that individuals know when and how they are affected by AI systems; safeguards for access to remedy; independent monitoring/oversight mechanisms ensuring that government agencies and business enterprises comply with relevant rules, etc.

For some time now there have been efforts at European level to build an appropriate legal framework that will address the issues of artificial intelligence application. Enacting the relevant framework that will address the risks and issues raised by daily application of artificial intelligence is becoming more and more crucial, in order to ensure that the development and use of intelligent systems proceeds in the same direction with the elaboration and enforcing of the relevant legal framework. Many European countries as well as the European Commission, the Council of Europe and several European Agencies, are developing strategies and programmes to guide the development of AI, with shared concerns over the need for an agreed ethical framework and applications that clearly benefit European society and uphold the European values enshrined in the Treaties. Most national strategies analyzed give similar attention to strengthening their research base, including the setting up of one or more national centers for AI, support for their industry, and SMEs, and awareness of the need to share data better between all the stakeholders: the public sector, industry, and the public. They also focus on applications

² Salom Lucas A. (2020) Artificial Intelligence and the future of Human Rights [in:] Florek I., Koroncziová A., Zamora Manzano J.L., Crisis as a challenge for human rights, Publisher Comenius University in Bratislava, p. 438. <https://doi.org/10.13166/mng/100020>

aimed at modernizing public administrations, as well as specific sectors such as health.³ Several European Countries such as France, Germany, Denmark and Austria have been particularly active in developing national strategic documents and policies on Artificial Intelligence, while there are initiatives in developing national AI strategies in most European Countries⁴.

In February 2017 the European Parliament adopted a report with recommendations to the Commission on Civil Law Rules on Robotics⁵. This report calls the European Commission (hereinafter referred to as “The commission”, or EC) to propose common Union definitions of cyber physical systems, autonomous systems, smart autonomous robots and their subcategories. In 2018, the Commission presented an AI strategy⁶ for the first time, and agreed a coordinated plan prepared with Member States to foster the development and use of AI in Europe. In the adopted strategy the European Commission put forward three strands that aim to place Europe ahead of technological developments and encourage the uptake of AI by the public and private sectors, prepare for socio-economic changes brought about by AI and ensure an appropriate ethical and legal framework. The coordinated plan proposes joint actions for closer and more efficient cooperation between Member States, Norway, Switzerland and the Commission in four key areas: increasing investment, making more data available, fostering talent and ensuring trust. Stronger coordination is essential for Europe to become the world-leading region for developing and deploying cutting-edge, ethical and secure AI⁷. The European Commission set ‘A Europe fit for the digital age’ as one of its 6 priorities for 2019-24, and launched several initiatives in that frame⁸. Furthermore, in 2020 the European Commission adopted a White Paper⁹ on artificial intelligence presenting the policy options regarding AI development in Europe in respect of the values and rights of EU citizens. The White Paper proposes: (1) new

³ http://www.aepia.org/aepia/files/Docs_interes_IA/ai-flagship-report_online-ilovepdf-compressed.pdf pp.43

⁴ Specific progress by country, link: https://knowledge4policy.ec.europa.eu/ai-watch_en#browse-ai%20watch-by-country

⁵ Please refer to the full text of the report, link: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html#def_1_1

⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN>

⁷ Link: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_6689

⁸ Link: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

⁹ Refer to the full text of the document, link: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

effective legislation on AI adapted to the risks but not limiting innovation; (2) transparent and traceable high-risk AI systems and under human control; (3) enable authorities to check AI systems as they check cosmetics, cars or toys to ensure that bias in data sets is appropriately addressed; (4) launch an EU-wide debate on the use of remote biometric identification (e.g. facial recognition). The White Paper considers “fundamental rights” throughout the text, and dedicates a section to the ‘Risks for fundamental rights, including personal data and privacy protection and nondiscrimination’. In October 2020 the European Parliament issued a resolution¹⁰ with recommendations to the Commission on a civil liability regime for artificial intelligence.

Assessing the impact of digital technologies on human rights, democracy and the rule of law has also been in the focus of the Council of Europe which has developed relevant legal instruments and Internet Governance strategies¹¹. An important step of the Council of Europe (CoE) Council of Ministers in this regard is also the adoption of the terms of reference of the Ad hoc Committee on Artificial Intelligence (CAHAI) in September 2019¹². This Committee will examine, on the basis of broad multi-stakeholder consultations, the feasibility and potential elements of a legal framework for the development, design and application of artificial intelligence, based on the Council of Europe’s standards on human rights, democracy and the rule of law. In September 2020, the Committee of Ministers approved the first progress report¹³, which details the progress achieved and includes reflections on working methods, synergy and complementarity with other relevant stakeholders and proposals for further action by the CAHAI by means of a robust and clear roadmap.

While the diverse applications of AI tend to enhance the quality of life and help humans to make sense of the world we live in, daily application of AI must guarantee processing data legally, fair treatment of citizens and the right to be aware that AI is used by informing where and how while ensuring the right decision. Some of the most common uses of AI include the areas of social welfare, marketing, law enforcement and health service. These intelligent systems apply different levels of automation, complexity, and impact

¹⁰ Link: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_EN.html

¹¹ Link: <https://rm.coe.int/internet-governance-strategy-2016-2019-updated-version-06-mar-2018/1680790ebe>

¹² Link: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016809737a1

¹³ Link: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016809ed062

on individuals or society. Said that, these areas are closely related to the daily activity of society and the individual, and thus artificial intelligence becomes tangible in the daily lives of each of us. The simple purpose of using it is to save time, increase efficiency, and use human resources as effectively as possible. While these intelligent systems serve to the common good, through their algorithms, there should be a very high level of awareness about the result. In this regard, there are several aspects of AI that are of concern. The preferences, the interests or the biases of those who write artificially intelligent programs may be reflected in the programs themselves. To some extent, this is unavoidable. However, this is particularly problematic in the context of AI, since AI tools can be so very powerful.

The increasing use of artificially intelligent technologies affects the theory and practice of law. The potential benefits of using AI manifest in the same time potential risks. While AI can be employed to optimize existing legal processes and allow law to be used in previously impossible ways, it is necessary to raise awareness of the wider social, ethical and legal implications of using AI.

Legal framework should come up with a meaningful way to acknowledge electronic persons so that in the future, we can actually hold machines responsible for what they do. The rise of intelligent autonomous machines and the legal challenges that they create, does not necessarily make legal regulation less relevant in this domain, but it does call for some legal engineering and for a great deal of legal ingenuity.