VANJA KORAĆ
Mathematical Institute SASA
11000 Belgrade, Serbia,
E-mail: vanja@mi.sanu.ac.rs

DRAGAN PRLJA
Institute for Comparative Law, Belgrade
11000 Belgrade, Serbia
E-mail: dprlja@gmail.com

GORDANA GASMI
Institute for Comparative Law, Belgrade
11000 Belgrade, Serbia
E-mail: gordana.gasmi@gmail.com

Received: September 14th 2021
Accepted: November 20th 2021
Original research article
004.8:341.24(4:497.11)"2021"
COBISS.SR-ID 55269641
https://doi.org/10.18485/arhe_apn.2021.17.10

CHALLENGES BROUGHT ON BY ARTIFICIAL INTELLIGENCE

ABSTRACT

The wide-spread use of artificial intelligence places in front of us numerous challenges, from those regarding individuals or pose a threat to human rights or cause algorithmic discrimination, to those that interfere with the obligations and legal security of producers of artificial intelligence systems, and even those that compromise the digital sovereignty of countries. A response to these challenges is the creation of mechanisms at a national and international level that would provide for the safe and controlled use of artificial intelligence systems. The proposal of the EU Artificial Intelligence Act, from April 2021, is a good example of how high-risk artificial intelligence systems can be controlled and safely managed.

KEYWORDS: ARTIFICIAL INTELLIGENCE, EUROPEAN UNION, HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEMS, HUMAN RIGHTS, ALGORITHMIC DISCRIMINATION.

Artificial intelligence represents a new step in the technological and scientific development that will have a huge influence on the manner in which the world as we know it functions (Andonović 2020: 142). Thanks to the great progress in terms of computer power, increasingly more sophisticated algorithms and the unprecedented amount of data, artificial intelligence has begun to create significant economic value. Due to the algorithms that perform predictions on the basis of large amounts of data, artificial intelligence, according to some estimates, contributes ca 2 billion dollars to today's global economy, and it can be expected that it will reach 16 trillion dollars by 2030, accounting for more than 10 percent of the gross world product (Stanton *et al*. 2019). Artificial intelligence systems comprehend software whose task is to generate output results, for a given set of goals, determined by human input, such as content, predictions, recommendations or decisions that affect the environment that the system is interacting with, either in a physical or digital dimension. They can be designed so as to work on different autonomy levels and be used independently or as an integral part of a given product, regardless of whether it is a system physically integrated into a product (built-in) or if it performs the function of a product without being integrated in it (not built-in). The software is developed on the basis of machine learning methods, or methods based on logics or knowledge, or on the basis of statistical approaches, a Bayes estimator, and

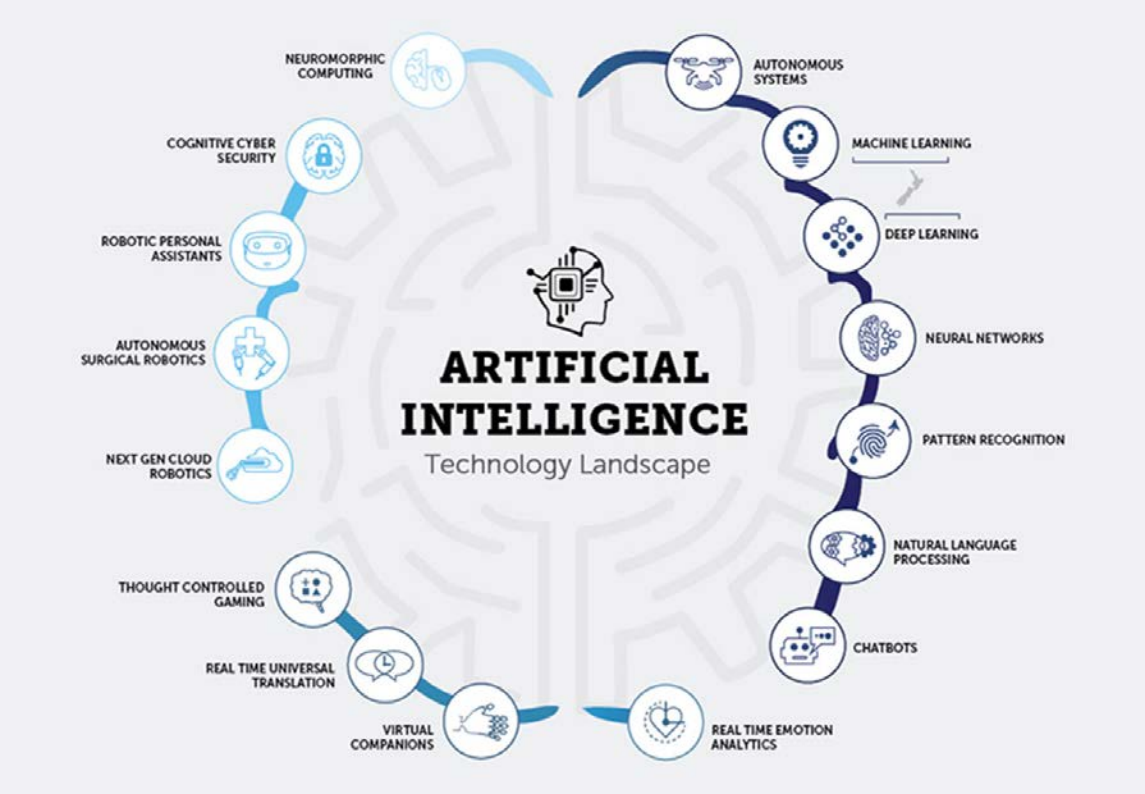

Fig. 1 Artificial Intelligence Technology Landscape (Ahmed N. A. 2021, What is Artificial Intelligence?, AI Time Journal, https://www.aitimejournal.com/@nisha.arya.ahmed/what-is-artificial-intelligence-ai)

search and optimisation methods.

Artificial intelligence systems can also be defined as algorithmic models that perform cognitive or perceptual functions (reasonable interpretation) that used to be reserved for thinking, judging and reasoning performed exclusively by humans (Leslie 2020: 8).

One of the more important traits of most artificial intelligence systems is that a large amount of data is needed to construct and run them. These large sets of data require large volumes of memory, and are used for revealing patterns and trends. The data can be numbers, words or images, and can be structured or unstructured. A specific science on data exists that deals with the manner of processing and analysing data and includes elements from different disciplines, such as informatics, mathematics, statistics, and social sciences.

The process of creating an artificial intelligence system comprehends several phases: planning, defining problems, data provision, data analysis, preliminary data processing, selecting models, testing models, implementation, users training, monitoring and controlling, and updating and correcting (Leslie 2020: 10–12). In the first phase of planning an artificial intelligence system, when the goals of the project are being defined, it is necessary to consider, aside from technical and economic issues, both ethical and legal issues as well. In the problem defining phase, a definition is made for the necessary input data, for what purpose it will be used and what the consequences of its use will be, including both the ethical and legal implications. Data provision is the phase in which the data is obtained via extraction from the internet, surveys, or by utilising already collected large amounts of data, by way of a contract with the owner of the data. Once the data has been provided, it must be analysed in detail in order to establish whether it is complete, whether there are discrepancies in terms of unexpected data, unbalanced data or missing data, and correlations must be established between the various pieces of data. In the phase of preliminary data processing, data cleansing, data transformation, the removal of incomplete data, and the conversion of data into formats suitable for use within the model are performed. The choice of artificial intelligence

Fig. 2 The Machine Learning Value Change
(Stanton C, et al. 2019, *What the Machine Learning Value Chain Means for Geopolitics,* https://carnegieendowment.org/2019/08/05/what-machine-learning-value-chain-means-for-geopolitics-pub-79631)

system models depends on the complexity of the problem that is to be solved, the type of data to be used, the amount and availability of data, whether it should be adapted and to what extent, etc. The testing of models is necessary in order to adapt them, since many models are based on learning, hence, it is necessary to verify the parameters within which the model learns are managed. For example, if models learn from earlier decisions that have caused discrimination based on gender, then new decisions will also cause that same discrimination. Control of the elements of the model architecture is also performed in this phase, so that they can be changed, if necessary, and the performance of the model itself can be improved. i.e. so that the number of errors is reduced. After the testing of an artificial intelligence model, and before it is implemented, it is necessary to evaluate the working of the model and to assess its impact, from its performance when working, to the risks that might occur, and it is necessary to carefully document it all. The next phase of the life cycle of an artificial intelligence system is its implementation, on the basis of new data, in order to achieve the purpose for which it was created. Users of artificial intelligence system have to be trained in order to understand the logic of the functioning of the system, so that they are able to autonomously assess and measure the quality and reliability of the results provided by the system. They should evaluate the system and indicate the qualities and shortcomings or dangers that can arise from its use. After the implementation of an artificial intelligence system, it must be further monitored in order to establish if it serves the desired purpose, if it is used in a responsible manner and to determine how it reacts to newly created conditions of use. The use of artificial intelligence systems can indicate the need for significant changes, at which time it may be necessary to perform additional designing, model changes, analyses, testing and controls.

The complexity of the life cycle of creating an artificial intelligence system is also followed by a large number of participants in the value chain of artificial intelligence. This chain comprehends all the participants who work together in order to meet the demand on the market for a particular product or service. At the bottom of this chain there are large amounts of data from which artificial intelligence systems are developed. Fast processing of this data requires powerful computers, with extremely fast chips and complex online platforms, which provide the necessary resources to producers of artificial intelligence systems so that they can test and verify their algorithms. At the end of the artificial intelligence chain there are companies that will distribute the artificial intelligence systems, in a commercial or non-commercial manner, and countries, which will create, individually or in cooperation with other countries, a safe environment for the application and control of artificial intelligence systems that are in use.

Products and services based on artificial intel-

ligence are in mass use today: autonomous vehicles, different types of robots, systems for biometric identification and categorisation of individuals, systems for traffic management, water supply, electricity supply, gas supply, heating, educational systems for grading and marking, systems for assessing credit ratings for individuals, artificial intelligence systems for hiring and managing workers, systems intended for public authorities for the approval of various services and forms of assistance, systems for judiciary and criminal prosecution authorities, systems for emergency services, systems for public authorities for controlling travel documents, visas, asylums, migrants, systems intended for democratic processes (electronic voting et al.), and many others. Their use provides optimisation of operations, better allocation of resources, improved predictions, personalisation of services provided, positive effects on the preservation of human lives and health, environmental protection, etc. The use of autonomous vehicles controlled by artificial intelligence will almost eliminate traffic accidents and human casualties in the future. These numerous positive effects brought about by the use of artificial intelligence are also accompanied by numerous challenges that affect individuals and pose a threat to human rights or cause algorithmic discrimination to users of these systems, threaten the legal security of producers of artificial intelligence systems, and can even pose a threat to the digital sovereignty of countries. The use of artificial intelligence systems can threaten the rights of individuals to dignity, respect for private life, data protection, non-discrimination, equality between women and men, freedom of expression and assembly, as well as the right to an effective legal remedy, fair trial and presumption of innocence, the right to good administration, fair and just working conditions, consumer rights, children's and persons with disabilities rights, and the right to environmental protection and to human health and safety.

The use of artificial intelligence systems in the judiciary can have a negative effect on the right to a fair trial if the decision is made using an algorithm, particularly if the judicial staff do not have a sufficiently high level of understanding of artificial intelligence to ensure that any decisions made with the use of it are non-discriminatory. Biometric face and voice recognition systems can threaten the right of individuals to privacy. Artificial intelligence systems that collect and analyse a large amount of data on individuals can potentially predict their behaviour, cause changes in their behaviour, and can compromise their privacy by revealing, for example, their facial expressions, emotional state, heart rate, physical location, etc. Biometric face recognition systems can prevent citizens from exercising their right to the freedom of expression, assembly and association and, thus, have a negative effect on social solidarity and participation in democratic processes. Chatbot activities and the creation of undoubtedly falsified content (Deep Fake) by a system based on an algorithm and artificial intelligence can affect the ability of individuals to form attitudes on reliable information, i.e. individuals can be manipulated and their right to be informed jeopardised, which is necessary in order for them to be able to take part in democratic decision making processes. Artificial intelligence systems based on biased information can cause algorithmic discrimination, i.e. discriminatory algorithmic decisions or behaviour. If an artificial intelligence system learns on the basis of preliminary data based on discriminatory decisions, then it can also, on the basis of "feedback loops", make discriminatory decisions, that is to say, it can threaten human rights.

Artificial intelligence systems intended for monitoring the behaviour of employees and making decisions using an algorithm can have negative effects on the realisation of the social and economic rights of employees. Employees can subsequently face errors committed by artificial intelligence systems, the consequence of which can be unjustly lower pay, unpaid holiday allowance, inadequate reassignment, etc. The consequence of an algorithm managing work processes can be dehumanisation and endangering the rights of the employees. All these reasons require serious consideration of the question of banning the use of certain artificial intelligence systems and controlling the more high-risk artificial intelligence systems.

International acts protecting human rights are first and foremost the UN Universal Declaration of Human Rights, from 1948; the European Convention on Human Rights, from 1950; the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social

and Cultural Rights of the UN, from 1966; the *Charter* of *Fundamental Rights* of *the EU, from* 2009, etc.

On the basis of these legal regulations, mechanisms have been created on a regional and national level that ensure the safe and controlled use of artificial intelligence systems. The proposal of the Artificial Intelligence Act of the EU, from April 2021, is a good example of how to safely manage and control high-risk artificial intelligence systems. The EU's approach to challenges originating from the use of artificial intelligence is based on the special treatment of high-risk artificial intelligence systems compared to those that do not fall into this category. Special rules and mechanisms for enforcing rules are established for those high-risk systems that pose a high risk to the health, safety and fundamental rights of individuals. The rules establish legal requirements regarding data and data management, documentation and record keeping, transparency and informing of users, human control, resilience, accuracy and safety regarding producers, importers, distributors, authorised representatives and users. It is foreseen that a European Committee on Artificial Intelligence be founded at the European Union level, and at the level of individual countries – bodies that would determine compliance with the requirements of the Act and appoint supervisory bodies.

The European Committee on Artificial Intelligence will consist of representatives of the member countries and the European Commission. National compliance assessment bodies will designate a competent national body, which will assess compliance with reliable quality management and risk management systems. Also, artificial intelligence systems will be monitored after reaching the market and certificates will be issued on their compliance with the requirements of the Act. The competent national body will control the application and heavily penalise producers who do not adhere to the prescribed provisions, with fines of up to 30 million Euros, or up to 6% of the total annual turnover of the given company worldwide for the previous fiscal year. In addition to these binding legal norms, the proposed mechanism of legal regulation foresees the creation of a code of conduct that would be voluntarily adhered to by the producers of high-risk artificial intelligence systems, as well as producers of artificial intelligence systems that are not in the high-risk group. The annexes of the proposal of the EU Artificial Intelligence Act define techniques and methods for harmonising artificial intelligence systems with regulations, list high-risk artificial intelligence systems, define obligations regarding technical documentation, as well as list the elements of the EU declaration of conformity. They also include the compliance assessment procedures on the basis of internal control, evaluation of the quality management system and evaluation of technical documentation. Additionally, the set of data that has to be submitted when registering high-risk artificial intelligence systems in the EU database managed by the European Commission is defined. In order to encourage innovation in the field of artificial intelligence, a controlled environment will be created for experimenting and testing in the development phase, before the artificial intelligence systems are placed on the market. The proposal of the EU Artificial Intelligence Act envisions the establishment of common rules for isolated environments for artificial intelligence with a special legal regime, first and foremost to aid small and medium sized companies and newly founded (start-up) companies. This way, a legal basis would be established for the use of personal data collected in order to develop specific AI systems of public interest in an isolated environment.

At a national level, member countries of the EU will be obliged to harmonise their legislation with the provisions of the Artificial Intelligence Act once it has been passed. It is expected that the Act will be passed at some point next year, in 2022, and its implementation is expected to begin in 2024. Countries aiming to become members of the EU are also expected to harmonise their legislation with the provisions of the Act and build mechanisms that will enable the safe use of high-risk artificial intelligence systems and ensure legal security. The complex legal framework requires the enactment of new regulations and amendments of existing regulations that have binding effects as well as those that do not. The first category will certainly include a special law on artificial intelligence with a strict sanctions mechanism, which will ensure efficient implementation. The experience with the General Data Protection Regulation (GDPR) has shown that sanctions with a high monetary value strongly influence the adher-

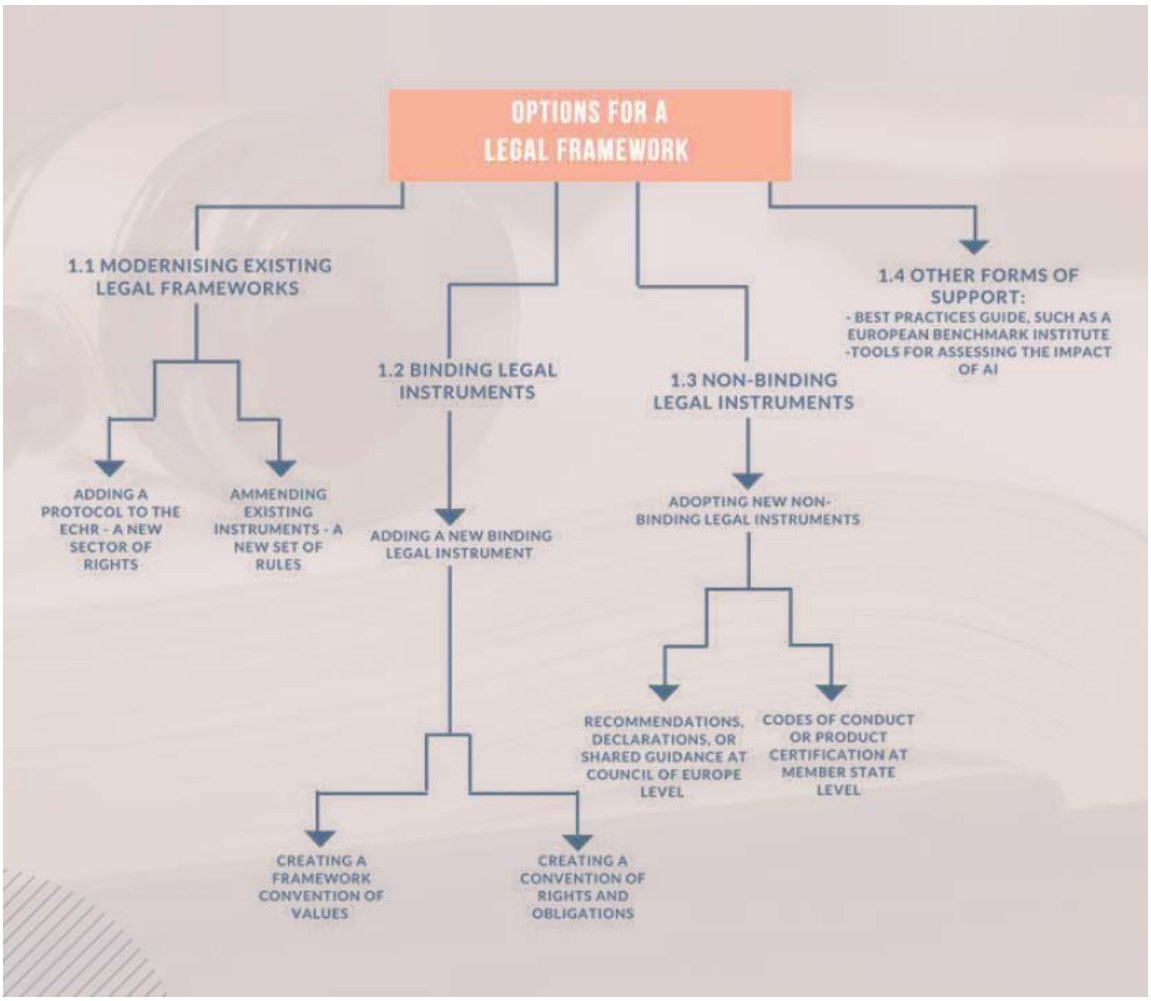

Fig. 3 Options for a Legal Framework
(Leslie, D. et al. 2021, Artificial Intelligence, Human Rights, Democracy, and Rule of Law: a Primer, The Council of Europe, https://rm.coe.int/primer-en-new-cover-pages-coe-english-compressed-2754-7186-0228-v-1/1680a2fd4a)

ence to legal regulations (Andonović i Prlja 2020: 120). The second category, that of non-binding regulations, includes professional codes of conduct at a national level and recommendations and declarations, primarily from international organisations such as the Council of Europe.

Artificial intelligence has and will have, without a shadow of doubt, a huge impact on the development of economy and society and all individuals as well. It brings numerous positive effects, but also dangers and risks as well. We must face this challenge by creating mechanisms for controlling high-risk artificial intelligence systems and ensuring their efficient application. The proposed EU Artificial Intelligence Act is certainly a positive step in this direction.

BIBLIOGRAPHY

Andonović, S. 2020
Normativni aspekti veštačke inteligencije u radu organa uprave u Republici Srbiji, u: *Usklađivanje pravnog sistema Srbije sa standardima EU*, ur. S. Soković, Kragujevac: Pravni fakultet, 142-154.

Andonović, S. i Prlja D. 2020
Osnovi prava zaštite podataka o ličnosti, Beograd: Institut za uporedno pravo.

Artificial Intelligence Act, 2021
Proposal for a Regulation of the European Parliamentandof the Council Laying Down Harmonised Ruleson Artificial Intelligence (Artificial intelligence Act) and Amendung CertainUnion

Legislative Acts, Brussels: European Commission, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

Leslie, D. et al. 2021
Artificial Intelligence, Human Rights, Democracy, and Rule of Law: a Primer, The Council of Europe, https://rm.coe.int/primer-en-new-cover-pages-coe-english-compressed-2754-7186-0228-v-1/1680a2fd4a

Stanton C, et al. 2019
What the Machine Learning Value Chain Means for Geopolitics, https://carnegieendowment.org/2019/08/05/what-machine-learning-value-chain-means-for-geopolitics-pub-79631

REZIME
IZAZOVI KOJE DONOSI VEŠTAČKA INTELIGENCIJA

KLJUČNE REČI: VEŠTAČKA INTELIGENCIJA, EVROPSKA UNIJA, VISOKORIZIČNI SISTEMI VEŠTAČK INTELIGENCIJA, LJUDSKA PRAVA, ALGORITAMSKA DISKRIMINACIJA

Raširena upotrebe veštačke inteligencije stavlja nas pred mnogobrojne izazove, od onih koji se odnose na pojedince i predstavljaju ugrožavanje ljudskih prava ili izazivaju algoritamsku diskriminaciju do onih koji zadiru u obaveze i pravnu sigurnost proizvođača sistema veštačke inteligencije, pa čak i do onih koji ugrožavaju digitalni suverenitet država. Odgovor ovim izazovima je stvaranje mehanizma na nacionalnom i međunarodnim nivou koji će obezbediti bezbednu i kontrolisanu upotrebu sistema veštačke inteligencije. Predlog Uredbe EU o veštačkoj inteligenciji iz aprila 2021. godine dobar je primer kako da se visokorizični sistemi veštačke inteligencije kontrolišu i bezbedno upotrebljavaju.

* * *