***Przegląd Europejski*, ISSN: 1641-2478**
vol. 2022, no. 3

DOI: https://doi.org/10.31338/1641-2478pe.3.22.4

Artificial intelligence *versus* human – a threat or a necessity of evolution?[1]

Izabela Oleksiewicz, *Ignacy Lukasiewicz Rzeszow University of Technology (Rzeszow, Poland)*
E-mail: oleiza@prz.edu.pl
ORCID ID: 0000-0002-1622-7467

Abstract
Currently, technologies are actively shaping and intensifying the time of implementation of artificial intelligence (AI) systems, while at the same time the so-called soft skills that employers are looking for in future employees are becoming increasingly important. Thus, in today's situation, we have the possibility to use automatons and robots that successfully replace humans in many tasks, while at the same time there is a need to create teams based on such qualities as empathy, communication, ingenuity, intelligence and, above all, humanism, whose importance in creating a business perspective cannot be overestimated. The aim of this article is to analyse the research problem in case of social robots and the probable legal status of artificial intelligence in the future. The article will discuss the differences between artificial intelligence *versus* artificial consciousness. AI poses societal challenges, it is currently undergoing a number of important developments, and the law must be rapidly changed. Firstly, the difference between artificial intelligence and artificial consciousness is attempted to be demystified. Subsequently, the analysis of current legal status of Artificial Intelligence in EU will be conducted. Cyberspace and the Internet revolutionised human life. It brings benefits, but also hitherto unknown risks. However, this is an inherent problem of human development. Every new technology, every new invention has its advantages, but also disadvantages. It would seem that autonomous systems, using artificial intelligence, are a panacea for such problems. Perhaps so, but the security of cyberspace depends on a variety of factors that are sometimes beyond our control or, from another perspective, we ourselves create the threat, inspire it intentionally or through inadequacies, ignorance, and negligence.
Keywords: artificial intelligence, human, threat, European Union, development

[1] This article was written in the framework of the project *Netzwerk für Sicherheits- und Konfliktforschung in Bayern* (NetKon).

Sztuczna inteligencja kontra człowiek – zagrożenie czy konieczność ewolucji?

Streszczenie

Obecnie technologie aktywnie kształtują i intensyfikują czas wdrażania systemów sztucznej inteligencji (AI), jednocześnie coraz większego znaczenia nabierają tzw. umiejętności miękkie, których pracodawcy poszukują u przyszłych pracowników. Tak więc w dzisiejszej sytuacji mamy możliwość wykorzystania automatów i robotów, które z powodzeniem zastępują człowieka w wielu zadaniach. Jednocześnie istnieje potrzeba tworzenia zespołów opartych na takich cechach jak empatia, komunikatywność, pomysłowość, inteligencja, a przede wszystkim humanizm, którego znaczenie w tworzeniu perspektywy biznesowej jest nie do przecenienia. W związku z powyższym, niniejszy artykuł ma na celu analizę problemu badawczego w przypadku robotów społecznych oraz prawdopodobnego statusu prawnego sztucznej inteligencji w przyszłości. W artykule zostaną pokazane różnice między sztuczną inteligencją a sztuczną świadomością, ponieważ AI stawia wyzwania społeczne, więc obecnie przechodzi szereg ważnych zmian i prawo musi być szybko zmienione. Po pierwsze, podjęto próbę demistyfikacji różnic między sztuczną inteligencją a sztuczną świadomością. Następnie analizie zostanie poddany aktualny stan prawny dotyczący sztucznej inteligencji w UE. Cyberprzestrzeń (w tym Internet) zrewolucjonizowała życie człowieka. Niesie korzyści, ale również nieznane dotąd zagrożenia. Jest to jednak nieodłączny problem rozwoju człowieka. Każda nowa technologia, każdy nowy wynalazek ma swoje zalety, ale i wady. Wydawać by się mogło, że autonomiczne systemy, wykorzystujące sztuczną inteligencję, są panaceum na takie problemy. Być może tak, ale bezpieczeństwo cyberprzestrzeni zależy od wielu czynników, na które czasem nie mamy wpływu, albo z innej perspektywy to my sami stwarzamy zagrożenie, inspirujemy je celowo lub przez niedociągnięcia, ignorancję i zaniedbanie.

Słowa kluczowe: sztuczna inteligencja, człowiek, zagrożenie, Unia Europejska, rozwój

Artificial intelligence (AI) commonly replaces advanced algorithm technology today. Thanks to AI, repetitive and relatively simple tasks that previously took a lot of time for skilled workers can be completed much faster. However, the standardisation of input data is a problem, if only because it has to be processed by programmes, whose syntax is predetermined, even if the algorithms have many possibilities for self-modification depending on changing processing rules and results. Only the creation of universal artificial general intelligence (AGI) will in any way reflect the capabilities of the human brain to perceive and process data. It will allow digital systems to be guided by the results of successive iterations of data processing, and it will also sometimes allow them to go against the results obtained, i.e. to take actions that are seemingly illogical from the point of view of previous experience (Iwankiewicz 2017: p. 36).

However, advanced algorithms capable of automation are increasingly entering various areas of our lives (e.g. see: Sitek et al. 2021), especially in business, including human resource management. The disadvantage of AI is, above all, its inability to study soft skills related to a human's personality, attitude, commitment and behaviour. Indeed, various attempts have been made in research institutes and technology company laboratories to digitally analyse the "body language" and facial expressions from recorded videos, but many mistakes can be made in extracting rules from unrelated material (Iwankiewicz 2018: p. 98).

The aim of this article is to analyse the legal status of artificial intelligence in EU and try to show its advantages and disadvantages. Firstly, it can be assumed that due to the continuous evolution of technology the speed, at which humans can process complex data, in addition to the fact that it comes from a variety of sources, will greatly speed up our decision-making process. On the other hand, the errors that can arise, cause raise the fear that decisions based on the results of such systems can lead us in unpredictable and even undesirable directions. An attempt will be made to answer the fundamental question of how far should the legal framework related to artificial intelligence be regulated, and is it moving in the right legal direction in the EU?

The evolution of artificial intelligence in the EU is developing in various areas of life. However, the development of AI raises a number of social and ethical issues, e.g. the relationship "between users and socially interactive robots may lead to psychological dependencies which are likely to be exploited by the companies creating these robots" (Oleksiewicz, Civelek 2019: s. 261). Research is therefore needed on the ethics and rights of robots in different environments, as similar issues arising in different cultures may have different results (Mamak 2017: p. 156; Scheutz 2012; Malle et al. 2015: s. 117–120). For example, Nick Bostrom points out that the level of artificial intelligence is steadily increasing and moving in a direction that goes even beyond the human level (Bostrom 2014: p. 76).

The evolution of artificial intelligence in the EU

The plan of building the information society, including AI, in the European Union was initiated in 1993[2] in the document *Growth, Competitiveness and Employment – The Challenges and Ways Forward into the 21st Century,* COM(93)700 final (see: European Commission 1993). This *White Paper* was focused mainly on economic issues, with priority given to the competitiveness of the European Community's economy and the achievement of IT standards developed by the United States. However, the publication in 1994 of the document *Europe and Global Information Society: Recommendations to the European Council* can be considered as the beginning of the development of the policy of creating the information society. This act was called the *Bangemann Report* – after Martin Bangemann, Commissioner for Industry, Information Technology and Telecommunications, and the demands it contained set out the European Union's policy in the field of information society.

On 24 July 1996, the Commission published the *Green Paper: Living and Working in Information Society,* COM(96)389 final (see: European Commission 1996). This document was focused on the consequences for citizens of the transformation towards the information society and the impact of ICT on their lives. Another initiative of the European Union aimed at building a modern and strong economy of the Member States was the *eEurope*

[2] The history of AI is much longer and dates back to the 1950s, and the current state of development of this technology is the third wave of interest in solutions of this nature. Only now – due to various factors – AI has become a widely used technology, which translates not only into the axiology of regulations, but also into the life of each of us.

– *An Information Society for All,* COM(1999)687 final (see: European Commission 1999a). In 1999, the *Green Paper of Public Sector Information: a Key Resource for Europe* was published (COM(1998)585 final, see: European Commission 1999b). This document described the benefits for both citizens and the entire economy that resulted from the use of telecommunications and information technologies in the area of public services.

During the European summit in Feira in 2000, another plan was adopted – *eEurope 2002 – An Information Society for All,* COM(2000)330 final (see: European Commission 2000). This document indicated the need to develop fast, cheap, universal Internet, invest in human potential and popularise the use of the virtual network. The next plan for the development of the information society, understood as a strategic element of building a knowledge-based economy, was presented in Gothenburg in 2001. In the document *eEurope 2003: A Co-operative Effort to Implement the Information Society in Europe – Action Plan*, it was assumed to accelerate reforms and stimulate the modernisation of the economies of candidate countries through the use of information society tools and technologies. One of the main goals was also to improve competitiveness and social cohesion. This initiative was also supported by the candidate countries to the European Union at that time.

On 21–22 June 2002, the European Union summit was held in Seville, during which a plan for the development of the information society till 2005 was adopted. In the document *eEurope 2005: An Information Society for All – An Action Plan,* COM(2002)263 final (see: European Commission 2002), the EU Member States undertook the following tasks:

- development of electronic services: e-learning, e-government, e-health;
- creating a dynamic environment for the development of the electronic economy; ensuring universal access to broadband Internet;
- building an information infrastructure security system.

The future of technology and the use of artificial intelligence and robotics seem to be a major threat, both in terms of people, work and social relationships. However, the future belongs not only to technology companies, but also to HR managers, who should:

- value the employee-company relationship so as to help employees feel respected and valued, which in turn strengthens their relationship with the company and develops their competencies, making them more engaged and productive;
- work on the company's image and brand, which is closely linked to the organisation's culture and strategy, and also involves the company's reputation, which is threatened by an unlimited amount of fake news about internal problems online and among current and future employees;
- improve operational efficiency, especially in responding to market crises, customer needs and working with all stakeholders, so that problems are resolved many times faster than before (Torczyńska 2019: p. 112; Leszkowska 2019: Szałkowska 2020).

Placing certain areas of activity in the hands of AI is undoubtedly a serious problem and will dehumanise cognitive processes and hinder human relationships. It may also

limit creativity in finding out-of-the-box solutions to different types of problems. Ultimately, algorithms, even those that can be automated, have one thing in common: they rely on the same raw data, process it in a certain way and ultimately produce repeatable results. In nature, the evolution of species and genetic errors often lead to anomalies that in some cases result in increased adaptation to the environment and in others in the degradation of entire populations.

The advantage of technology is that it is independent of its environment. It doesn't act under the influence of emotions, it doesn't have bad or worse days, it simply acts as it was built and programmed to act. Therefore, although I am personally sceptical about the introduction of AI-based solutions, I see many benefits. On the one hand, it can significantly speed up the decision-making process, as the speed of human processing is unattainable in the face of complex data from different sources, not understood by humans. On the other hand, errors that can occur for trivial reasons (also occurring at a technical level, e.g. processor structure, algorithm structure, device wear and tear, data sets fed into the system, etc.) (Garrison, Hamilton 2019: p. 99–114) can lead us in unpredictable and even undesirable directions when decisions based on the results obtained from these systems.

Human *versus* robot

Human rights are conceptualised as real relationships, which are understood in a variety of ways in different fields of human activities, including state law (Oleksiewicz 2021: p. 343–348). Sometimes, in constitutional terminology, the same individual rights are considered as rights at one time and as freedoms at another time, which is not without significance and legal consequences for the persons exercising them. An individual's freedom does not, in fact, derive from legal acts, i.e. a subjective right (Bógdał-Brzezińska 2020: p.135).

The law does not confer them, but only defines the limits of their application. It is the task of the state to protect and guarantee human freedom. The characteristic feature of freedom is that the state and its organs are obliged to refrain from acting in the spheres of life covered by a particular freedom.

Most commonly, individual freedom is understood as a category of the individual's entitlements, which is intended to secure the individual's sphere of privacy. In the sphere defined as freedom, the individual is entitled to make decisions, behaviour and actions motivated by his or her own will and, most importantly, it is a zone free from state interference, thus it is an asset protected by law. Moreover, it is not without foundation that freedoms are considered to be the guarantee of the other entitlements, since only a free person can enjoy the fullness of his or her rights (Pagallo 2013: p. 47–66).

Today, the value system that permeates the consciousness of almost all inhabitants of the globe is human rights and freedoms. The process of the universalisation of human rights, for which the milestones were such events as the French Revolution and the achievements of the American Revolution, accelerated in the 20th century

with the adoption of the *United Nations Charter* (see: United Nations WWW) and the creation of the UN.[3]

One of the main objectives set for the new organisation besides the preservation of international security and peace – was the protection of human rights. This was not possible under the conditions of a bipolar world, when one pole of this arrangement massively violated the rights of individuals and whole peoples, treating them as an invention of Western imperialism (Dela 2020: p. 98). The erosion of such a position came with the development of the CSCE process, in which the West, in exchange for political and economic concessions, forced the USSR and the socialist countries to respect human rights more and to have greater freedom in terms of travel, flow of ideas and information. The breakthrough, however, came only after the collapse of the USSR and the fall of communism. Human rights grew to become a universal value, the basis for the functioning of democratic societies, and their protection framed by the international regime in global, regional and national dimensions.

Restrictions on privacy and individual freedom are a permanent feature of contemporary politics and economics. This problem is nowadays primarily associated with the widespread practice of *General Data Protection Regulation* (see: Regulation (EU) 2016/679). However, it should be borne in mind that "the accumulation of personal data in the hands of companies and government institutions and agencies poses a threat to our freedom, not only online, but also to civil liberty more broadly" (Mróz 2017: p. 147), without which there can be no real implementation of the ideals of freedom and social equality. Very often, these are joined by doubts of an emotional nature. They have their deep "roots" stemming from a sense of uncertainty and perhaps even from fear or emotions associated with the novelty and puzzling nature of a new situation for the ordinary person. Reasons of an emotional nature are generally linked to the fact that people generally react strongly negatively to the possibility of losing their specific monopoly on intelligence, which determined their unique position in the hitherto organisation of the world (Mirski 2000: p. 93–97). As A. Mirski argues, man as a rational being does not want to be deprived of *ratio* or *cognito* (Mirski 2000: p. 97). The most pessimistic attitudes are linked to a deep-seated fear of the results of the decisions and actions of, out of human control, intelligent machines (e. g. see: Schellekens 2021). The spectre of the irreversible consequences of the actions of "autonomous" intelligent machines (exploited, for example, by the film industry in countless variations on the theme of the "robot revolt") cannot be ignored. In such context, extreme negative emotions about artificial intelligence are often formed.

The danger will arise when the systems themselves start modifying the goals of their actions, which would not have been possible even when they became self-aware. For a long time, only one message from AI experts has reached the public, according to which computers cannot set themselves tasks without first finding a justification for them. Artificial intelligence as a new technology can also pose risks to the person using it

[3] The UN came into being on 24 October 1945 as a result of the entry into force of the *Charter of the United Nations* signed in San Francisco on 26 June 1945. The UN is the successor to the League of Nations.

and to bystanders; autonomous cars can be particularly dangerous for the environment and the AI user, if the autonomous vehicle's sensors fail to identify an object in its path or the AI misinterprets the environment or the situation and causes an accident. The risk of an accident, can occur due to a faulty AI system, with the quality of the information collected by the AI, or other problems arising from the functioning of the AI system in a given facility. The lack of appropriate regulations and the lack of competences and adequate resources for the market surveillance authorities may result in a lower overall level of safety and an uncertain situation for the companies putting IS into operation in the EU. All the aspects presented in the emergence of an accident make it difficult to detect and trace decisions made by AI affecting the course of an incident, which may translate into complications for the victim in obtaining compensation (COM(2020)65 final, see: European Commission 2020b: p. 14–15).

Another threat posed by the development of artificial intelligence, raised by Bill Gates, Elon Musk and Stephen Hawking, among others, is the emergence of super-intelligence, or AI, which will be able to continuously and autonomously improve itself. In this way, it will not only surpass the level of humans, but will reach a level of uncontrollable development, with its motives remaining unguessed (Fehler 2017: p. 73). Warning against the irresponsible development of AI systems, Stephen Hawking stated in October 2016 that "we spend a lot of time studying history, which is mainly the history of stupidity, rather than thinking about the future of intelligence".[4] In their concerns, Hawking or Musk emphasise that thinking machines could be used to create dangerous weapons and to increase the level of exploitation of some people by others. In the opinion of the aforementioned researcher, the emergence of full artificial intelligence could spell the end of the human race, although today the achievements of human brains augmented with AI systems cannot be predicted. They point out that it is in fact difficult to imagine the extent, to which AI can contribute to the well-being of society, but it is equally difficult to predict the extent of the dangers should someone want to build AI systems or use them inappropriately.

Legal basis for AI in the European Union

Artificial intelligence, as a technological solution, does not have legal capacity for the time being and cannot be held liable for damages caused by its functioning in the current state of the law. An important issue in this area has always been the legal status of artificial intelligence in the European Union. For this purpose, it was assumed that the evolution of artificial intelligence in the EU is developing in various areas of life. Nevertheless the improvement of AI can result in many social and moral issues, e.g. the relationship among customers and socially interactive robots might also additionally cause mental dependencies that probably can be exploited by corporations developing such robots. Nick Bostrom suggests that the extent of synthetic intelligence

[4] About future possibilities – e.g. see: Oleksiewicz, Civelek 2019: p. 260–261.

is systematically growing and is moving in a course that is going beyond the human level (Bostrom 2014: p. 76).

On 16 February 2017 the European Parliament issued a resolution with recommendations to the Commission on civil law, entitled: *Rules on Robotics* (O.J. C 252/239, 18.07.2018). The resolution was drafted with a view to making full use of the provisions regarding the field of ethics and security policy, in particular artificial intelligence. Among the solutions, there was also a proposal to establish the legal status of AI. The resolution proposed to give robots a special status – known as electronic person status or simply granting them the personality of legal persons. Electronic person status can be described as the basis for another form of personhood in law, with the proviso of establishing a new form of legal personhood in the long term. This legal status would apply to the most developed AI systems. The objective of granting electronic person status to entities such as AI has been the subject of scientific and legal discussion for years, and is based on the basis for the independent liability for damages of robots (Report from the Expert Group on Liability and New Technologies – New Technologies Formation, see: European Commission 2019).

The result of this joint work was the publication on 25 April 2018 by the Commission the communication *Artificial Intelligence for Europe* COM(2018)237 final (see: European Commission 2018a) outlining an *EU Initiative on AI* (or the *Artificial Intelligence Strategy*). It was then endorsed by the European Council in June 2018. Its purposes were:

1) Boosting the EU's technological and industrial capacity and AI uptake across the economy;
2) Preparing for socio-economic changes brought about by AI;
3) Ensuring an appropriate ethical and legal framework, based on the Union's values and in line with the Charter of Fundamental Rights of the European Union (European Commission 2018a: p. 3).

The next step was the adoption by the European Commission on 7 December 2018 of the *Coordinated Plan on Artificial Intelligence,* COM(2018)795 final (see: European Commission 2018b).

The individual actions started in 2019–2020. A further confirmation of the actions was the adoption of the *White Paper on Artificial Intelligence – A European approach to excellence and trust,* COM(2020)65 final, on 19 February 2020 (see: European Commission 2020b). Artificial intelligence, connecting diverse technological fields, has had to be modified and adapted by many sectors of global industries and economies, and in doing so is seen as a front for innovation and enabling technology (Campbell 1986: p. 5–7). Artificial intelligence consists of a comprehensive set of computational techniques for extracting "insights from a variety of data sources, including so-called 'small data' generated by the algorithm itself, that assist in decision-making" (Teece 2018: p. 1370–1372; qtd. in: Xu et al. 2019) and produce useful information. Artificial intelligence is considered as "a general-purpose technology that can have significant technological, social, economic and political implications" (Xu et al. 2019).

Growing cyber threats and perceptions of cyber insecurity were causing increased distrust among citizens, potentially holding back the European economy as it becomes

digitalised. The *Digital Single Market Strategy for Europe* (COM(2015)192 final, 6 May 2015) reiterated the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (JOIN(2013)1 final, 7 February 2013). The aim of the *EU Cybersecurity Strategy* was to establish common minimum requirements for network and information security between Member States.

The European Commission recognised the cybersecurity as a key element of the market strategy. The reform was to be based on the actions envisaged in the cyber security strategy and the main pillar of the strategy – the Directive (EU) 2016/1148 (also known as *Network and Information Systems Directive*, or *NIS Directive*). This directive created an EU-wide cyber-security regime, which aim is, among other things, to ensure the uninterrupted provision of key services and incident handling by achieving an adequate level of security of the information systems used to provide these services. The *NIS Directive* obliged all EU Member States to guarantee a minimum level of national capabilities in the field of cyber security by establishing competent authorities and a single point of contact for cyber security, the establishment of teams of Computer Security Incident Response Teams (CSIRTs) and the adoption of national cyber-security strategies (see also: Dąbrowski 2022: p. 105–106; Directive (EU) 2022/2555).[5]

In April 2019, The Council adopted a regulation known as the *Cybersecurity Act* (see: Regulation (EU) 2019/881), which established an EU-level certification scheme and a modernised EU cyber-security agency ENISA. It also established legislation to impose EU targeted mitigation and sanctions measures to prevent and respond to cyber-attacks that pose an external threat to the Union or its Member States. As a part of the same reform, the EU also introduced legislation to establish a *European Cyber Security Research and Competence Centre* supported by a network of national coordination centres. These structures will help secure the Digital Single Market and increase EU autonomy in the field of cyber security. In addition, the EU can impose sanctions against EU persons or entities, as well as against non-EU countries or international organisations, if it deems it necessary to achieve the objectives of the *Common Foreign and Security Policy* (see: Regulation (EU) 2019/881). An important move in cyber-security policy was the release of the *2020 White Paper on Artificial Intelligence*, which is expected to be key to combating cyber-terrorism and achieving climate governance by improving AI. This is a necessary element to maintain the EU single market through research, innovation and the implementation of a coordinated roadmap under the programmes *Digital Europe* and *Horizon Europe* for 2021–2027 from December 2020. The latest step under the aforementioned programme is the establishment of the Joint Cyber Unit on 4 August 2021. Its role was to develop till 31 December 2021 the *EU Cybersecurity Incident and Crisis Response Plan*, based on national plans. It was intended that the *EU Cybersecurity Incident and Crisis Response Plan* will set out the procedure and information sharing, as well as the criteria for triggering the mutual assistance mechanism based

[5] On 14 December 2022 the new Directive (EU) 2022/2555 of the European Parliament and of the Council was adopted, co-called *NIS 2 Directive*, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

on an agreed classification of incidents and a list of available EU capabilities (Council of the European Union 2021).

On 21 April 2021, a draft Regulation of the European Parliament and of the Council of the EU was published, concerning the creation and adoption of harmonised legal standards for artificial intelligence systems in the European Union. From the content of the draft, we can learn that AI, as a rapidly developing technology that can bring a number of economic and social benefits, can also give rise to risks for humans or society. At the same time, the EU wants to ensure that new technologies are developed and used in accordance with the core values of human rights and the fundamental principles of the organisation. It is these elements that have guided the Commission's work in drafting the Regulation. It is also a continuation of the Union's work in previous years, such as the publication of the *2018 European Strategy on Artificial Intelligence* and the *2020 White Paper on Artificial Intelligence*.

In light of the existing regulations, also an invention must have an inventor, who is a specific individual. This is, as recognised in legal doctrine, a person who has contributed to the invention by making an intellectual contribution that goes beyond routine technical or organisational assistance. In the past, there were concepts of the fiction of invention without an inventor, the so-called company invention or enterprise invention (Danish, USSR, Romanian concept). However, this idea has disappeared and is now incompatible with the provisions of the Paris Convention for the Protection of Industrial Property (Abbott 2016: p. 1085; Konieczna 2019: p. 109–112).

Some experts point out that in the US, for example, the law requires less of a human factor to grant protection for IP rights, which may harm the competitiveness of European companies.

It is important to remember that the process of managing research and development projects takes into account not only the possibility of implementing a solution and generating revenue from specific products or services. Sometimes an equally important asset is intellectual property rights, which can be licensed or sold alone or in packages, or simply protected by exclusive rights against competition. If the subject matter of the intellectual property (this is especially true for computer programmes and inventions) is not a human creation, it will not be protected under the current state of the law and will not fit into the traditional Research & Development strategy model. A law allowing the protection of inventions or works created autonomously by machines seems desirable from the point of view of current technological development.

Conclusions

The aim of this article was the analysis of the legal status of artificial intelligence in the EU, as well as showing its advantages and disadvantage. The question that has been bothering science for years, where is the legal borderline of regulation between AI and human, has primarily two dimensions: ethical and legal, where the inadequacy of current legal regulations in relation to civil and criminal liability, legal subjectivity, copyright is raised,

and the operation of AI is considered in the context of personal data protection, which the author tried to demonstrate in the aspect of the revolution represented by cyberspace.

First of all, artificial intelligence can provide many benefits to citizens, businesses and society as a whole, on condition that it is human-centred, sustainable, and it respects fundamental values. We must remember that the damage it can cause can be both tangible and intangible and can include many different risks.

Secondly, that is why the main EU regulatory framework should be focused on how to minimise the various risks associated with the potential harms, especially the most serious ones. The main risks associated with AI are related to the application of regulations to protect fundamental rights such as data protection and privacy law, non-discrimination, security and liability issues (Bose 2017: p. 2268–2270).

Thirdly, AI offers important efficiency and productivity benefits that can strengthen the competitiveness of European industry. It can also contribute to finding solutions to some of the most pressing societal challenges, including those related to combating climate change and environmental degradation, challenges related to sustainable development and demographic change, and the protection of democracy, as well as contributing to the fight against crime, if necessary, and in a proportionate manner.

Fourthly, Europe should take full advantage of the opportunities offered by AI, but it needs to develop and strengthen the necessary industrial and technological capabilities. As set out in the *European Strategy for Data* (COM(2020)66 final, 19 February 2020, see: European Commission 2020a) accompanying the *White Paper on Artificial Intelligence – A European approach to excellence and trust* (COM(2020)65 final, 19 February 2020, see: European Commission 2020b), this also requires measures to enable the EU to become a global data centre.

Fifth, AI can perform many functions that previously only humans could perform. As a result, citizens and legal entities are increasingly subject of the actions and decisions made by AI or with the help of artificial intelligence systems, which can sometimes be difficult to understand and change when necessary (European Commission 2020b: p. 11). AI also enhances the ability to monitor and analyse everyday human behaviour. Artificial intelligence also enhances the ability for monitoring and analysing everyday human behaviour at different levels of the EU airport screening system. Algorithms that autonomously recognise behaviour that betray stress, affective states and emotional arousal could revolutionise not only security checks carried out against possible threats to public safety (e.g. countering terrorist attacks), but also improve the detection of customs crime, such as that related to the smuggling of prohibited goods (e.g. drugs, weapons, foreign currency, counterfeit goods, items prohibited under CITES) and illegal migration of persons. These types of solutions not only have the potential to significantly increase the level of European security in passenger air transport, but also have a human side: they improve the comfort of air travelling, increase passenger satisfaction, minimise time loss and stress associated with activities involving uniformed, armed and often not very polite security officers, and reduce the workload of staff and liability for possible errors and omissions (Biscop 2019).

Sixth, AI can be used by government agencies, other mass surveillance agencies and employers who monitor the behaviour of their employees in breach of EU data protection and other laws. The data being processed and the potential for human intervention may affect rights to privacy, freedom of expression, data protection, and political freedoms.

The ability of artificial intelligence to think and make decisions on its own raises concerns for people. Doubts and fears are being raised that humans will be unfit for most jobs, that they will exploit human bodies, or that they will ignore the value of human life. These fears seem unfounded, as there is no indication that humans will be able to create not only intelligent machines, but also machines with consciousness and personality. Such problems always arise when dealing with completely new technologies.

Izabela Oleksiewicz – PhD, D.Sc., university professor at the *Ignacy Lukasiewicz Rzeszow University of Technology* (Department of Law and Administration). An expert at the *Center for Doctrine and Training of the Armed Forces* in the NUP 2X35 analytical project on cybersecurity in the area of information impact on society and state security policy and law. Its result is the current *National Strategy of the Republic of Poland*. Earlier she was the manager of the international project *Cybersecurity in Poland and Germany* as a part of *Mobilität 2018_2* no. MB-2018-2/3 by BAYHOST (germ. *Bayerisches Hochschulzentrum für Mittel-, Ost- und Südosteuropa*). She is also participating in the international project *Netzwerk für Sicherheits- und Konfliktforschung in Bayern* (NetKon) from 01.07.2022 to 30.06.2024 in the area of digitisation and security, which will result in the creating new research network. Research interests: anti-terrorism policy, cyber security, refugees as a threat to the European Union area. Recent published monographs: *Polityka antyterrorystyczna i uchodźcza jako wyzwanie Unii Europejskiej w XXI w.* (Warszawa 2018); *Ochrona cyberprzestrzeni. Polityka–strategia–prawo* (Warszawa 2021).

Izabela Oleksiewicz – dr hab., profesor Politechniki Rzeszowskiej (Katedra Prawa i Administracji). Ekspert Centrum Doktryny i Szkolenia Sił Zbrojnych w projekcie analitycznym NUP 2X35 dotyczącym cyberbezpieczeństwa w obszarze wpływu informacji na społeczeństwo oraz politykę i prawo bezpieczeństwa państwa. Efektem projektu jest aktualna *Strategia Narodowa Rzeczypospolitej Polskiej*. Wcześniej autorka była kierownikiem międzynarodowego projektu *Cyberbezpieczeństwo w Polsce i Niemczech* w ramach *Mobilität 2018_2* nr MB-2018-2/3 realizowanego przez BAYHOST (niem. *Bayerisches Hochschulzentrum für Mittel-, Ost- und Südosteuropa*). Uczestniczy również w międzynarodowym projekcie *Netzwerk für Sicherheits- und Konfliktforschung in Bayern* (NetKon) od 01.07.2022 do 30.06.2024 w obszarze digitalizacji i bezpieczeństwa, którego efektem będzie utworzenie nowej sieci badawczej. Zainteresowania badawcze: polityka antyterrorystyczna, cyberbezpieczeństwo, uchodźcy jako zagrożenie dla obszaru Unii Europejskiej. Ostatnio opublikowane monografie: *Polityka antyterrorystyczna i uchodźcza jako wyzwanie Unii Europejskiej w XXI w.* (Warszawa 2018); *Ochrona cyberprzestrzeni. Polityka–strategia–prawo* (Warszawa 2021).

References:

ABBOTT Ryan (2016), *I Think, Therefore I Invent: Creative Computers and the Future of Patent Law*, „Boston College Law Review", vol. 57, issue 4.

BISCOP Sven (2019), *The EU Global Strategy 2020,* "Security Policy Brief", no.108, EGMONT – Royal Institute for International Relations, Brussels, https://www.egmontinstitute.be/app/uploads/2019/03/SPB108.pdf?type=pdf (31.03.2019).

BOSE Bimal K. (2017), *Artificial Intelligence Techniques in Smart Grid and Renewable Energy Systems – Some Example Applications*, „Proceedings of the IEEE", vol. 105. DOI: 10.1109/JPROC.2017.2756596

BOSTROM Nick (2014), *Superintelligence. Paths, Dangers, Strategies*, Oxford.

BÓGDAŁ-BRZEZIŃSKA Agnieszka (2020), *Cyberprzestrzeń i przestrzeń kosmiczna jako sfery bezpieczeństwa międzynarodowego – aspekty teoretyczne,* in: M. Jurgilewicz, M. Delong, K. Michalski, W. Krztoń (eds), *Wyzwania bezpieczeństwa w XXI w.*, Rzeszów.

CAMPBELL John A. (1986), *On artificial intelligence*, „Artificial Intelligence Review", vol. 1, no. 1.

COUNCIL OF THE EUROPEAN UNION (2021), Council Conclusions on exploring the potential of the Joint Cyber Unit initiative – complementing the EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises – Approval, 12534/21, Brussels, 08.10.2021.

DĄBROWSKI Hieronim (2022), *Dostarczanie usług cyfrowych i cyberbezpieczeństwo na gruncie Dyrektywy NIS i aktów ją wdrażających w Republice Malty oraz w Rzeczypospolitej Polskiej*, „Przegląd Europejski" no. 2/2022. DOI: 10.31338/1641-2478pe.2.22.6

DELA Piotr (2020), *Teoria walki w cyberprzestrzeni*, Warszawa.

DIRECTIVE (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.07.2016.

DIRECTIVE (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), PE/32/2022/REV/2, OJ L 333, 27.12.2022.

EUROPEAN COMMISSION (1993), *White Paper on growth, competitiveness, and employment – The challenges and ways forward into 21st century*, COM(93) 700 final, Brussels, 05.12.1993.

EUROPEAN COMMISSION (1996), Green Paper: *Living and Working in Information Society: People first,* COM(96) 389 final, Brussels, 24.07.1996.

EUROPEAN COMMISSION (1999a), *eEurope – An Information Society for All* – Communication on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000, COM(1999) 687 final, Brussels, 08.12.1999.

EUROPEAN COMMISSION (1999b), *Public sector information: a key resource for Europe* – Green Paper on public sector information in the information society, COM(1998)585 final, Brussels, 20.01.1999.

EUROPEAN COMMISSION (2000), *eEurope 2002 – An Information Society for All* – Draft Action Plan prepared by the European Commission for the European Council in Feira – 19-20 June 2000, COM(2000) 330 final, Brussels, 24.05.2000.

EUROPEAN COMMISSION (2002), Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – *eEurope 2005: An information society for all* – An Action Plan to be presented in view of the Sevilla European Council, 21/22 June 2002, COM(2002) 263 final, Brussels, 28.05.2002.

EUROPEAN COMMISSION (2013), Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *Cybersecurity Stra-*

tegy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final, Brussels, 07.02.2013.

EUROPEAN COMMISSION (2015), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *A Digital Single Market Strategy for Europe*, COM(2015) 192 final, Brussels, 06.05.2015.

EUROPEAN COMMISSION (2018a), Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: *Artificial Intelligence for Europe*, COM(2018) 237 final, Brussels, 25.04.2018.

EUROPEAN COMMISSION (2018b), Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: *Coordinated Plan on Artificial Intelligence,* COM(2018) 795 final, Brussels, 07.12.2018.

EUROPEAN COMMISSION (2019), *Liability for Artificial Intelligence and Other Emerging Digital Technologies*, Report from the Expert Group on Liability and New Technologies – New Technologies Formation, DOI: 10.2838/573689

EUROPEAN COMMISSION (2020a), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *A European strategy for data,* COM(2020) 66 final, Brussels, 19.02.2020.

EUROPEAN COMMISSION (2020b), *White Paper on Artificial Intelligence – A European approach to excellence and trust,* COM(2020) 65 final, Brussels, 19.02.2020.

EUROPEAN PARLIAMENT (2018), European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law *Rules on Robotics* (2015/2103(INL)), OJ C 252, 18.07.2018.

FEHLER Włodzimierz (2017), *Sztuczna inteligencja – szansa czy zagrożenie*?, „Studia Bobolanum", vol. 28, no. 3.

GARRISON Chlotia, HAMILTON Clovia (2019), *A comparative analysis of the EU GDPR to the US's breach notifications*, „Information & Communications Technology Law", vol. 28, issue 1. DOI: 10.1080 /13600834.2019.1571473

IWANKIEWICZ Maciej (2017), *Robot też człowiek*, „Personel Plus", no. 8 (117).

IWANKIEWICZ Maciej (2018), *Robot, czyli ten lepszy*, „Personel Plus", no. 2 (123).

KONIECZNA Agata (2019), *Problematyka sztucznej inteligencji w świetle prawa autorskiego*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Prawa Własności Intelektualnej", no. 4.

LESZKOWSKA Anna (2019), *Sztuczna inteligencja a prawo*, „Sprawy Nauki", no. 6-7.

MALLE Bertram F., SCHEUTZ Matthias, ARNOLD Thomas, VOIKLIS John, CUSIMANO Corey (2015), *Sacrifice One for the Good of Many? People Apply Different Moral Norms to Human and Robot Agents*, "HRI'15: Proceedings of the Tenth Annual ACM (IEEE International Conference on Human-Robot Interaction". DOI: 10.1145/2696454.2696458

MAMAK Kamil (2017), *Prawo karne przyszłości*, Warszawa.

MIRSKI Andrzej (2000), *Inteligencja naturalna a sztuczna, czyli inteligencja podmiotu i przedmiotu* [in:] E. Szumakowicz (ed.), *Granice sztucznej inteligencji. Eseje i studia*, Kraków.

MRÓZ Bogdan (2017), *Konsument a wyzwania technologiczne XXI wieku*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach", no. 330.

OLEKSIEWICZ Izabela, CIVELEK Mustafa Emre (2019), *From Artificial Intelligence to Artificial Consciousness: possible legal bases for the human-robot relationships in the future,* „International Journal of Advanced Research", no. 7(3). DOI: 10.21474/IJAR01/8629

OLEKSIEWICZ Izabela (2021), *Ochrona cyberprzestrzeni Unii Europejskiej. Polityka – Strategia – Prawo,* Warszawa.

PAGALLO Ugo (2013), *The Laws of Robots: Crimes, Contracts, and Torts*, Springer.

REGULATION 2016/679 of the European Parliament and of the EU Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 04.05.2016.

REGULATION (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 07.06.2019.

SCHELLEKENS Jasper (2021), *Release the bots of war: social media and Artificial Intelligence as international cyber attack*, "Przegląd Europejski", no. 4/2021. DOI: 10.31338/1641-2478pe.4.21.10

SCHEUTZ Matthias (2012), *The Inherent Dangers of Unidirectional Emotional Bonds between Humans and Social Robots*, in: Patrick Lin, Keith Abney, George A. Bekey (Eds.), *Robot ethics: the ethical and social implications of robotics*, Cambridge.

SITEK Anna, GRESER Jarosław, KNIEĆ Wojciech, WAGSTAFF Anthony, KAUTSCH Marcin, MARTINEZ-PEREZ Jonatan (2021), *The effect of the pandemics on e-health services in Poland*, "Zdrowie Publiczne i Zarządzanie", vol. 19, no. 2. DOI: 10.4467/20842627OZ.21.006.15760

SZAŁKOWSKA Joanna (2020), *7 grzechów głównych AI, czyli dlaczego potrzebujemy etycznej sztucznej inteligencji,* „Homo Digital", https://homodigital.pl/sztuczna-inteligencja-7-grzechow-glownych-ai/ (24.11.2020).

TEECE David J. (2018), *Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world*, „Research Policy", vol. 47, issue 8. DOI: 10.1016/j.respol.2017.01.015

TORCZYŃSKA Monika (2019), *Sztuczna inteligencja i jej społeczno-kulturowe implikacje w codziennym* życiu, „Historia i Kultura", no. 2.

TFEU, Treaty on the Functioning of the European Union (consolidated version), OJ C 202, 07.06.2016.

TREATY OF LISBON (2007) amending the *Treaty* on European Union and the Treaty establishing the European Community, signed at *Lisbon*, 13 December 2007, OJ C 306, 17.12.2007.

UNITED NATIONS (WWW), *United Nations Charter*, https://www.un.org/en/about-us/un-charter (03.09.2022).

XU Yueqiang, AHOKANGAS Petri, LOUIS Jean-Nicolas, PONGRÁCZ Eva (2019), *Electricity Market Empowered by Artificial Intelligence: A Platform Approach*, "Energies", vol. 12, issue 21. DOI: 10.3390/en12214128

Received: 03.09.2022. Accepted: 29.12.2022.