УДК 347.5:004.4
DOI: 10.37635/jnalsu.27(4).2020.185-198

Марина Миколаївна Великанова

Кафедра міжнародних відносин
Київський національний університет культури і мистецтв
Київ, Україна

ШТУЧНИЙ ІНТЕЛЕКТ: ПРАВОВІ ПРОБЛЕМИ ТА РИЗИКИ

Анотація. *Використання цифрових технологій та штучного інтелекту є реаліями сьогодення. Беззаперечною є значна кількість переваг, що надає штучний інтелект – це і зменшення витрат, ресурсів, часу, швидкий аналіз великих обсягів даних, збільшення продуктивності діяльності, побудова точніших прогнозів в різних сферах життєдіяльності, можливість одночасного виконання багатьох задач та ін. Втім, використання штучного інтелекту також супроводжується й низкою правових проблем та ризиків, що може обернутися завданням шкоди. Тому метою цієї публікації є виявлення правових проблем використання штучного інтелекту та окреслення підходів до розподілу ризиків, пов'язаних із використанням штучного інтелекту. У статті на підставі системного аналізу з використанням діалектичного, порівняльного, логічно-догматичного та інших методів окреслюються проблемні ситуації, що виникають у зв'язку з використанням штучного інтелекту та пропонуються окремі напрями їх вирішення. Зокрема серед проблем використання штучного інтелекту називаються: визначення особи, відповідальної за шкоду, завдану штучним інтелектом; прогалини у нормативно-правовому регулюванні відносин у сфері використання цифрових технологій, що ускладнює захист прав та законних інтересів фізичних та юридичних осіб; неможливість у багатьох випадках застосування чинних правил притягнення до цивільно-правової відповідальності за шкоду, завдану використанням штучного інтелекту. Напрямами вирішення таких проблем можуть бути: визначення статусу електронних осіб та окреслення їх правосуб'єктності, моменту її виникнення та припинення з одночасним вирішенням питання ідентифікації роботів та штучного інтелекту; вирішення питання відповідальності за шкоду, завдану штучним інтелектом, виходячи з того наскільки такий штучний інтелект був автономним; застосування правил відшкодування шкоди, завданої джерелом підвищеної небезпеки, до відносин із використанням цифрових технологій, виходячи з того, чи була шкода, завдана дією чи бездіяльністю штучного інтелекту, передбачуваною.*

Ключові слова: делікт, відповідальність, цивільне право, цифрові технології, конфіденційність.

Maryna M. Velykanova

Department of International Relations
Kyiv National University of Culture and Arts
Kyiv, Ukraine

ARTIFICIAL INTELLIGENCE: LEGAL PROBLEMS AND RISKS

Abstract. *The use of digital technologies and artificial intelligence are today's realities. Undoubtedly, there are many advantages of artificial intelligence – it reduces costs, resources, and time for rapid analysis of large amounts of data, an increase in productivity, making more*

accurate forecasts in various spheres of life, the ability to simultaneously perform many tasks and more. However, the use of artificial intelligence is also accompanied by several legal problems and risks, which can result in damage. Therefore, the purpose of this paper is to identify legal problems in the use of artificial intelligence and to outline approaches to the distribution of risks associated with the use of artificial intelligence. The paper, based on systems analysis using dialectical, comparative, logical-dogmatic and other approaches, outlines the problem situations that arise in connection with the use of artificial intelligence and suggests ways to solve them. In particular, among the problems of using artificial intelligence are listed: identification of the person responsible for the damage caused by artificial intelligence; gaps in the legal regulation of relations in the use of digital technologies, which complicates the protection of the rights and legitimate interests of individuals and legal entities; the impossibility in many cases of applying the current rules of civil liability for damage caused by the use of artificial intelligence. The directions for solving such problems can be: determination of the status of electronic persons and their legal personality, the moment of its occurrence and termination while addressing the issue of identification of robots and artificial intelligence; resolving the issue of liability for damage caused by artificial intelligence, based on how autonomous such artificial intelligence was; the application of the rules of compensation for damage caused by a source of increased danger to the relationship with the use of digital technologies, based on whether the damage caused by the action or inaction of artificial intelligence was predictable.

Keywords: tort, liability, civil law, digital technologies, confidentiality.

INTRODUCTION

In recent years, the concept of "artificial intelligence" has come into use and taken root in human life. Today it is quite difficult to imagine the existence without social networks, e-banking, various applications used on the Internet and as applications for smartphones. Such Internet activity is simply impossible without the use of highly developed systems capable of analysing certain conditions and making autonomous decisions in a certain way, which is artificial intelligence in a broad sense. Technology and artificial intelligence are critical in all aspects of responding to the COVID-19 crisis. Artificial intelligence (AI) tools and systems can help countries respond to the COVID-19 crisis. However, to make the most of innovative solutions, AI systems need to be designed, developed and applied reliably. They must respect human rights and confidentiality; be transparent, explainable, reliable and secure; and participants involved in their development and use must remain accountable[1].

There is a large number of definitions of "artificial intelligence" and approaches to understanding its essence – from identification with robotics to the perception of AI as an innovative direction in the development of science and technology aimed at creating intelligent machines and intelligent computer software. According to M.O. Stefanchuk, AI is essentially the ability of machines to learn from human experience and perform human-like tasks. It is a modelling of the ability to abstract, creative thinking – and especially the ability to learn – using digital computer logic [1]. The Oxford Dictionary defines artificial intelligence as the theory and development of computer systems capable of performing tasks that normally require human intelligence, such as visual perception,

[1] Recommendation of the Council on Artificial Intelligence. (2019, May). Retrived from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

language recognition, decision making, and translation between languages [2]. According to Amit Tyagi, AI is an imitation of human-like behaviour, such as learning, planning, reasoning, problem solving, environmental perception, natural language processing, etc. [3]

The essence of artificial intelligence was explained in the most detail by A.A. Baranov, noting "AI carries out processing (transformation) of input information by algorithms that implement the functions of the human brain and knowledge, pre-embedded in AI or acquired by it in the process of self-development, into new information that can play a role or direct informational impact to control some processes or perform the role of source information for a new (next) stage of information processing. Thus, AI is a set of software and hardware methods, tools (computer programmes) that implement one or more cognitive functions equivalent to the corresponding cognitive functions of a person" [4]. The attitude of the scientific community and the public to AI is also ambiguous. Admittedly, Elon Musk, Stephen Hawking, Bill Gates warned against the development of artificial intelligence, considering it a threat to humans. For example, Elon Musk once compared AI to the dangers of the dictator of North Korea [5]. Instead, Mark Zuckerberg points to the benefits for all mankind in the use of artificial intelligence. According to him, artificial intelligence will help humanity cope with many problems: people will be able to receive better treatment, diagnose diseases, reduce the number of accidents (which is currently the most common cause of death) [6]. For example, as noted by Chen X., Chen J., Cheng G., Gong T., AI is already used to predict people's reactions to decisions, including their perception or rejection [7].

The April 9, 2018 IEEE Confluence Report on AI and ML Applied to Cybersecurity states that the worst challenges for the future of AI are likely to be social in nature. Although AI promises to improve security by automating some aspects of defence, caution is needed in the design, deployment, and use of these systems. AI can cause irreversible damage to national security, economic stability and other social structures if not designed and used very carefully. Security networks with legal and ethical restrictions are required. It is necessary to build a social, ethical, and legal context that would prepare the world for the introduction of AI as well as the creation of technical systems themselves [8]. After all, as noted by Stephen Hawking, everything that is not forbidden can happen and will happen someday [9]. Therefore, there is an urgent need to outline the legal problems of using artificial intelligence and its inherent risks and work out ways to overcome them.

The purpose of this paper is to identify the legal problems of using artificial intelligence and to outline approaches to the distribution of risks associated with the use of artificial intelligence.

1. MATERIALS AND METHODS

Any study is aimed at acquiring theoretical knowledge, which in turn makes it possible to identify the essential, main properties of the object under study and separate them from secondary, random features. This is possible only with the use of appropriate methods. As noted by S.V. Vyshnovetska "... it is important not only to determine the subject of study, but also to find appropriate ways, methods and techniques by which this subject is covered" [10]. One of these techniques is systems analysis, the methodological basis of

which is dialectics. It is designed for systematic study of relevant issues, provided that a particular system (object) is considered as a whole, taking into account its goals and functions, structure, all external and internal connections. According to systems theory, the surrounding world is known as a set of systems of different complexity and different levels that interact with each other. Any object arises and exists within a certain large system, and the connections between objects and the system are the essential foundations of the origin, existence and development of the object and the system as a whole.

A system is a set of elements that are in certain relationships and connections with each other, interact with each other, form certain integrity and as a whole interact with the external environment. And at the same time the system is a set of means for solving problems. In this case, based on the provisions of systems theory, the problem always arises in a particular system. The dialectic of problem solving is that by solving one problem, one changes the system. The new system contains a new problem. In some cases, this problem is not significant and it can be assumed that the second system solves a problem for the first system. The next steps are aimed at solving the problem of the second system, which leads to another new system. Therefore, the system is considered as a set of means to solve the problem. The application of such an approach provides a systematic knowledge of problem situations that arise in connection with the use of artificial intelligence and the development of directions for their solution. Based on a systems analysis, the damage by artificial intelligence is considered as an element, an integral part of tortious obligations to compensate for damage. The issue of determining the place of artificial intelligence in the structure of civil matters is studied in the plane of systems of objects and subjects of such legal relations. At the same time, it is established that the introduction of artificial intelligence as an element of a system leads to certain problems. The development of an adequate theory of solving such problems should become the task of the science of civil law, the solution of which depends on the right goal and adequately chosen means. This led to the use of structural analysis, which establishes the relationship between the components of their impact on the environment – the general rule of law.

The use of the logical-dogmatic method along with the method of hermeneutics made it possible to consider the essence of the concept of "artificial intelligence" through the prism of its perception by interstate institutions and researchers. In particular, such methods were used to interpret the concept of "smart autonomous robots" through the analysis of the European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics and the scientific literature.

Using the analogue approach, it was hypothesised that the damage caused by artificial intelligence can be compensated according to the rules of compensation for damage caused by a source of increased danger. And the comparative approach allowed to clarify this hypothesis. Thus, having established the essence of the concepts of "infliction of harm by artificial intelligence" and "infliction of harm by a source of increased danger" and found differences between them. It was concluded that damage caused by artificial intelligence cannot always be compensated by the rules of compensation for damage caused by a source of increased danger, as it may have signs of unpredictability.

2. RESULTS AND DISCUSSION

2.1 Legal problems and risks of using artificial intelligence

In June 2019, the G20 Ministerial Statement on Trade and the Digital Economy was adopted, stating that innovative digital technologies continue to offer enormous economic opportunities. At the same time, they create challenges. The benefits of increased productivity through the use of new technologies such as artificial intelligence (AI), fifth generation mobile telecommunications technology (5G), Internet of Things (IoT), Distributed Ledger Technologies (e.g. blockchain) will expand the opportunities of individuals and legal entities, creating new opportunities, services and employment, which can lead to greater well-being and further inclusion of these people. However, while digitalisation has a huge potential to benefit society, it is also a matter of concern. Digitalisation issues include privacy, data protection, intellectual property rights and security issues [11]. This is especially true for the healthcare sector, where the personal data of many patients are collected [12]. Although, as noted by W. Nicholson Price II, AI can play at least four major roles in the health care system: pushing the boundaries of human activity (for example, Google Health has developed a programme that can predict the onset of acute kidney injury two days before trauma will occur, which is impossible for current medical practice, as the damage is often noticed only after it has happened [13]); democratisation of medical knowledge and excellence; automation of heavy work in medical practice; management of patients and medical resources [14].

The literature also suggests that the key area where artificial intelligence problems and risks are observed, in addition to information in the form of data and personal data, is language. In particular, issues related to privacy, data protection, are issues related to the quality of information, aspects of its creation, dissemination, updating and language barrier. This concerns the programme's understanding of the user's query, the search for meanings in verbal constructions, the division into semantic tuples for the formulation of phrases and their natural use. The language problem is primarily related to the processing of natural language. This is especially relevant for Ukraine, as on various platforms and sites there is no option to automatically create Ukrainian subtitles (for video) or translate the site into Ukrainian, recognition of spoken Ukrainian. The situation with the protection of personal data, which is an integral part of the information privacy of each person, is not better [15; 16].

Indeed, the collection and processing of personal information that is publicly available is a problem of great concern today. All users of social networks have repeatedly encountered cases of targeted advertising, which often has signs of discrimination. For example, a woman's profile feed often advertises tools, materials, information resources, webinars related to pregnancy and childcare, cooking, while a man's profile advertises watches, cars, yachts, and more. There are also cases of discrimination on the basis of skin colour, when for people with light skin colour luxury items are offered, and for dark skinned people – fast food. Now property discrimination is spreading, in particular, iPhone users with the Apple iOS operating system complain that when ordering a taxi, the cost of travel for them under the same conditions and for the same distance is higher than for users of phones with other operating systems, such as Android. Therefore, the need to protect personal data comes to the fore, and especially

from persons who collect personal information on a commercial basis for analysis and sale to companies that target or provide services. The McKinsey Global Institute's November 28, 2017 report, "Jobs lost, jobs gained: What the future of work will mean for jobs, skills, and wages" points to another problem with the use of artificial intelligence. In particular, it is noted that by 2030, from 400 to 800 million people worldwide may lose their jobs due to automation. Of this number, 75 to 375 million may need to change occupational categories and learn new skills according to the middle and earliest automation scenarios [17]. Instead, Oleksiy Reznichenko, the founder and head of the Boteon Robotics Centers network, told Radio Svoboda that although there are many automation tools that have replaced a lot of human labour, people still find work. The possibilities of AI are endless, the speed is incredible, the ability to combine and synchronise with a million more such robots, or to produce a million more such programmes – is endless, so here everything depends on people. There is a threat of hacker interference in the work of "smart" robots. It is the person who manages artificial intelligence on the first principles and robots – this is the greatest danger to other people" [6].

Daniel Larimer, CTO of EOS startup Block.one, sees the risk of using artificial intelligence as a possibility of total censorship, noting that recent blockades of cryptocurrency videos on YouTube indicate that powerful corporations are plunging the world into total censorship. In his opinion, it should be taken for granted that people do not own anything and do not control anything on their phone. Software will increasingly only be available for exclusive access [4]. Susanne Hupfer also points out the difficulties in managing the risks associated with AI [18], due to the fact that they cannot be reliably calculated [19]. Such risks, for example, may be that, when hiring and lending, AI may increase historical bias against women candidates and members of minorities or lead to non-transparent decisions [20]. Whether in the field of AI health care, using data collected by academic medical centres, there is less "knowledge" about patients from groups of the population who do not usually visit academic medical centres, and therefore will treat them less effectively. Similarly, if speech recognition systems are used to decipher patient appointment notes, the AI may perform worse, especially if the provider has a race or gender that is underrepresented in the training set [21]. Some scientists point out that the widespread use of AI will eventually reduce human knowledge and capabilities, as a result of which providers will lose the ability to detect and correct AI errors and further develop medical knowledge [22].

Another problem that stands in the way of effective use of artificial intelligence is the lack of necessary digital skills in many people and the backlog of legal regulation of the use of digital technologies [23]. In particular, as noted by I.V. Ponkin and A.I. Redkina on the inadequacy of regulatory regulation of the use of AI, insufficient attention on the part of the state to the use of AI as a new rapidly evolving technology can lead to loud disputes, critical technical failures and even causing death [24].

There is also the problem of determining the place of artificial intelligence in the structure of civil law. As noted by M.O. Stefanchuk, there are three main approaches to determining the legal status of robots (and artificial intelligence): 1) the perception of them exclusively as objects of civil law, which should be subject to the legal regime of things; 2) their perception exclusively as subjects of civil legal relations, holders of

subjective rights and responsibilities, who are able to act independently and to realise and evaluate the significance of their actions and the actions of others; 3) differentiated definition of the place of robots in the structure of civil relations, when they can be both subjects of civil relations and objects. In this case, according to the scientist, the most balanced is the third approach, which is primarily due to the technical capabilities of the robot as a carrier of artificial intelligence. That is, the attribution of a robot to the subject or object of civil law depends on how high a level of intelligence and autonomy it has and whether it can act independently and realise the importance of its actions [1].

In general, the problems of AI use and development are formulated in a generalised way in the report of the research group of Stanford University "Artificial Intelligence and Life in 2030". In particular, this report points to: problems of ensuring the confidentiality of personal information; problems of developing an effective policy in the field of innovation development; problems of civil and criminal prosecution; problems of determining the legal personality of the AI system, in particular in which situations the AI can act as an intermediary of a natural or legal person, enter into contracts; problems of certification of AI systems when using them to solve problems that, otherwise, require competent professionals whose activities are licensed by the state; the problem of the negative impact of the use of AI systems on the number of jobs for people [25].

The lack of an unambiguous understanding of the very category of "artificial intelligence" does not add certainty to its use. There are at least a few dozen different definitions of AI, grouped into four categories: think human, act human, think rationally, and act rationally [26]. However, the attempt of scientists to define the concept of AI by analogy with human intelligence does not improve the situation, because, as indicated by O.A. Baranov, representatives of various branches of knowledge characterise human intelligence not by one sign, but by a certain set of various properties (functions). Moreover, a stable, generally accepted definition of neither the actual cognitive function nor their list, which are taken as signs of human intelligence, has not yet been formed in science [4].

Thus, along with the advantages of using artificial intelligence, it is important to state a number of problems, the solution of which should become a priority for scientists and the state. Such problems are the problem of determining the place of artificial intelligence in the structure of civil law, gaps in the legal regulation of digital technology, ensuring the protection of the rights and legitimate interests of individuals and legal entities from violations of digital technology, prosecution for damage caused by digital technology. Let us try to outline some areas for solving such problems.

2.2 Approaches to the distribution of risks of using artificial intelligence

The High Level Group of Experts on the EU AI Development Strategy in April 2018, noting that trusted AI must respect all relevant laws and regulations, has developed seven key requirements for AI: 1) mediation and supervision of human activities: AI systems should ensure just societies while upholding human rights and fundamental rights, not reducing or restricting human decision-making rights; 2) reliability and security: algorithms must be stable, reliable and sufficient to eliminate errors or inconsistencies during all phases of the life cycle of AI systems; 3) confidentiality and data management: citizens should have full control over their own data, while data concerning them should not be used to harm or discriminate against them; 4) transparency: traceability of AI systems must be ensured; 5) diversity, non-discrimination and equity: AI systems must

take into account the full range of human abilities, skills and requirements and ensure accessibility; 6) social and environmental well-being: AI systems should be used to enhance positive social change and increase environmental responsibility; 7) accountability: mechanisms should be put in place to ensure accountability for AI systems and their results [27]. Taking into account these principles, the authors will outline some areas for solving problems related to the use of artificial intelligence.

Determining the place of artificial intelligence in the structure of civil law directly depends on what it means by "artificial intelligence". Today, as already noted, there is no single understanding of this category. Moreover, it is suggested that in the absence of a generally accepted definition of of artificial intelligence, it is appropriate to describe it through distinctive features, which include the ability to learn and make decisions independently. O.A. Baranov adds another feature – simulation (modelling, performance) of functions equivalent to human cognitive functions, to which he includes the perception, memory, exchange, analysis, comparison, evaluation, generalisation, and use of information (data) to solve problems or make decisions, recognition of objects and their classification (gnosis), choice of strategy and specific actions, expert assessment of the situation, goal setting, planning, text-to-speech and vice versa, self-learning, self-organisation, generating new knowledge, etc. [4]. Therefore, the problem of understanding AI as a subject (quasi-subject) or object of legal relations needs to be solved, as determining the place of AI in the structure of civil matters will answer the question of the possibility of applying the relevant rules of civil liability.

In the European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics in paragraph 59 suggests the idea of creating a specific legal status for robots, so that complex autonomous robots can be defined as having the status of electronic persons responsible for redressing the harm they can cause. It is also possible to use the status of an electronic person in situations where robots make autonomous decisions or interact independently with third parties. In this case, the term "smart autonomous robot" is proposed to mean technologies that have the following characteristics: 1) the ability to gain autonomy through sensors and/or by exchanging data with the environment and analyse this data; 2) the ability to learn through experience and interaction; 3) the form of physical support of the robot; 4) the ability to adapt their behaviour and actions to the environment; 5) lack of life in the biological sense. To track robots, it is proposed to introduce a system of registration of advanced robots based on the criteria established for their classification[1].

In general, the idea is quite progressive. Based on the trends in the development of science, including in the field of robotics and AI, sooner or later humanity will face the need to determine the status of intelligent robots and AI. And, as an option, it can be the status of an electronic person. In this case, giving robots and AI such a status, it is necessary to take the next step and recognise them as subjects (quasi-subjects) of legal relations, including subjects of civil liability. Accordingly, based on the current rules, compensation for damage should be relied on such electronic persons. And here logically there is a question of a way and sources of compensation of the caused damage. It is obvious that the traditional rules of civil liability are not able to solve this issue.

[1] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics. (2017, February). Retrieved from https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html?redirect.

Therefore, recognising AI as an independent subject of legal relations, at the same time it is necessary to resolve the issue of bringing to legal responsibility for the damage caused by AI. It is possible that the recognition of intelligent robots and AI as subjects of legal relations implies endowing them with a certain legal personality – the ability to have and acquire appropriate rights and responsibilities. Then civil liability, as the ability to bear adverse consequences, including property, will be covered by their legal personality. But it is necessary to outline the legal personality of electronic persons, as well as the moment of its occurrence and termination. The issue of identification of such robots and AI will also be urgent.

However, it should be noted that the understanding of AI as a subject (quasi-subject) of legal relations, including in the context of electronic persons, is only a prospect. Currently, given the current state of development of robotics and artificial intelligence, it is not time to talk about the prevalence of intelligent autonomous robots. Therefore, it is now more appropriate to consider robots and AI as objects of legal relations. Although in this case, the question of liability for damage still remains open. Thus, in the already mentioned Resolution of the European Parliament, it is stated that in the case where the robot can make autonomous decisions, there are difficulties in determining the party responsible for providing compensation. This applies both to contractual liability, where machines select contractors, agree on contractual terms, conclude contracts and decide whether and how to perform them, and cases of non-contractual liability, as Directive 85/374/EEC can only cover damage caused by manufacturing defects of robot, provided that the victim will be able to prove the actual damage, the defect of the product and the causal link between the damage and the defect. On the other hand, the damage caused by next-generation robots does not quite fall within the scope of this Directive, as such robots may be equipped with adaptive and learning abilities that cause a certain degree of unpredictability in their behaviour. Therefore, these robots will learn independently from their own experience and interact with the environment in a unique and unpredictable way. Accordingly, the rules of strict liability or liability without fault will not be able to resolve such a situation[1].

There is also no consensus among researchers on the principles of responsibility for the use of AI. For example, O.M. Vinnyk proposes, firstly, to legalise a person who uses AI by registering in the relevant register. Secondly, to hold accountable for damage caused by AI, to carry out: "a) for the use of AI – by analogy with the responsibility for the use of a source of increased danger, because all the consequences of AI use are difficult to predict, as well as ensuring 100% control over it; b) for unfair (in violation of the law, rights and legitimate interests of users/consumers) use of the site for business activities, responsibility should be assigned: as a general rule – the owner or person using the site for business activities (if it can be identified); if the participants of the virtual enterprise use one electronic resource/site, the principle of responsibility should be determined in the agreement on joint activities concluded between them and, accordingly, on the joint use of the site (the actual user defined in the agreement with the site owner), and in the absence of such agreement – the responsibility should rest with the owner of the site or its actual user, registered in the relevant register" [23].

[1] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics. (2017, February). Retrieved from https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html?redirect.

Unfortunately, the problem of determining the subject of responsibility was left without attention in the case when, by analogy, responsibility for the use of a source of increased danger is applied. According to the legislation of Ukraine, compensation for damage caused by a source of increased danger is entrusted to a person who on the appropriate legal basis (ownership rights, other property rights, contract, lease, etc.) owns a vehicle, mechanism, other object, the use, storage or the content of which creates an increased danger (Part 2 of Article 1187 of the Civil Code of Ukraine)[1]. It is also allowed to impose the obligation to compensate for such damage to several entities in cases of misappropriation of a vehicle, mechanism, other object and due to the interaction of several sources of increased danger (Part 4 of Article 1187, Article 1188 of the Civil Code of Ukraine)[2]. And according to Article 5:101 of Principles of European Tort Law[3], strict liability for damage caused by activities that are highly dangerous is borne by the person whose activities are associated with increased danger. In this case, the activity that creates an increased danger to others is recognised as such activity that: a) is characterised by the infliction of alleged and significant damage, regardless of whether the necessary precautions were taken to prevent it or not and b) is not generally accepted. This raises the question of the subject of responsibility for the harm caused by AI.

European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics[4] notes that A. Azimov's laws (1) a robot cannot cause harm to a person, or by its inaction allow a person to be harmed; 2) the robot must obey human orders, except for those that contradict the first law; 3) the robot must protect itself, unless its actions do not contradict the first and second laws. The author later added a zero law, according to which a robot cannot harm humanity or by its inaction allow humanity to be harmed) should be considered as aimed at engineers, manufacturers, and operators of robots, including robots, which are designed for built-in autonomy and self-learning, because these laws cannot be converted into machine code. Accordingly, in order for those involved in the development and commercialisation of AI programmes to develop safety and ethics from the outset, they must be prepared to take legal responsibility for the quality of the technology they produce. That is, it is the responsibility of engineers, manufacturers, and operators of robots. However, as noted by D.D. Pozova, the Resolution does not provide an unambiguous answer to the question of defining the range of responsible persons and does not contain a clearly defined concept of responsibility, setting out only the basic principles according to which such a concept should be developed and the factors to be taken into account [28].

It is considered that the determination of the person who should be liable for the damage caused by AI should be made on the basis of who caused the action or inaction of the AI, as a result of which the damage was caused. Thus, if the cause of the damage was, for example, an error in the programme code, and this, according to experts in the

[1] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15.
[2] *Ibidem*, 2003.
[3] Principles of European Tort Law: Text and Commentary. (2005, January). Retrived from https://www.researchgate.net/publication/321568630_Principles_of_European_Tort_Law_Text_and_Commentary.
[4] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics. (2017, February). Retrieved from https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html?redirect.

field of IT, occurs in the vast majority of cases, the responsibility for causing damage to AI should rest with software developers. But, aware of the existing risks, developers try to shift responsibility to users through a license agreement with the end user. The standard end user license agreement contains general terms, terms of use under the agreement, license to use and permissible use of the service, user guarantees under the agreement, license to use user content, restrictions on use. Without compromising the importance of such a license agreement, as it can be an effective means of protecting software developers from unscrupulous users, it is advisable to pay attention to a number of issues related to such an agreement. First, it is common among users to automatically agree to such a license agreement, when in order to install and use a particular programme, the user ticks in the "I agree" window, mostly without reading the terms of the agreement. This is, of course, the responsibility of the users themselves. However, perhaps by analogy with credit relationships, software developers need to pay special attention to their responsibilities and the consequences of non-compliance. Secondly, quite often the agreement states that it can be changed by the administration without any special notice to the user. In this case, the new version of the agreement, as a rule, comes into force from the moment of its placement on the website of the administration or bringing to the notice of the user in another convenient form, unless otherwise provided by the new version of the agreement. This, in turn, allows developers to shift responsibility for damage caused by the software to users at any time by amending the license agreement with the end user. In this case, it is advisable to establish the obligation of the developer to prove the fact of personal information to the user about changes in the license agreement. That is, the user must still receive a special message stating what exactly changes in the license agreement or use of the programme.

Based on the above, it is appropriate to support the position that the determination of the person who will be liable for the damage caused to AI depends on how autonomous such AI was. In other words, civil liability should be carried out in accordance with and in proportion to the actual level of instructions given in accordance with the degree of autonomy of the AI. Non-autonomous or partially autonomous robots should be considered as tools used by the subjects of legal relations – manufacturer, owner, software developer, user, public authority, military commander, etc. Accordingly, in this case, the responsibility for the damage or negative consequences should be placed in proportion to the developers of robots, their owners and users [29].

It is also worth agreeing with the opinion expressed in the scientific literature that compensation for damage caused by AI, according to the rules of compensation for damage caused by a source of increased danger, does not quite correspond to the essence of such a relationship [30]. It should be borne in mind that when it comes to compensation for damage caused by a source of increased danger, the infliction of such damage occurs in the case of using a particular vehicle, mechanism, equipment, which, although can get out of control, but not able to take autonomous decision. Instead, the feature of AI is its ability to make decisions independently. Consequently, the point is not in its uncontrollability, but also the unpredictability of its actions and causing harm. Accordingly, since such damage is unpredictable, its infliction is not covered by the concept of activities that pose an increased danger to others, in the sense of the Principles of European Tort Law. Therefore, in answering the question whether the damage caused by AI can be compensated according to the rules of compensation for damage caused by

a source of increased danger, it is necessary to determine not only the person who caused the action or inaction of AI, which resulted in damage, but also whether such damage is predictable. If such damage was not predictable, then the application of these rules does not seem possible.

CONCLUSIONS

Total digitalisation of all spheres of human life, the use of innovative digital technologies has a number of advantages: reduced costs, resources, time for information processing, rapid analysis of large amounts of data, increased productivity, more accurate forecasts in various spheres of life and more. This stimulates the more rapid development of such technologies, which results in the improvement of artificial intelligence. However, along with the undeniable advantages of such technologies, it is necessary to state a number of risks associated with the use of artificial intelligence. In particular, the uncertainty of the place of artificial intelligence in the structure of civil law raises the problem of determining the person responsible for the damage caused by artificial intelligence. Gaps in the legal regulation of the use of digital technologies, ensuring the protection of the rights and legitimate interests of individuals and legal entities from violations with the use of digital technologies and holding accountable for the harm caused by the use of digital technologies, creates the impossibility of compensation for damage, since the current rules cannot always be applied. Accordingly, the solution of these problems lies in the modernisation of current legislation in the following areas: 1) determining the status of electronic persons and outlining their legal personality, the moment of its occurrence and termination, solving the problem of identification of robots and artificial intelligence; 2) addressing the issue of liability for damage caused by artificial intelligence, based on how autonomous such artificial intelligence was; 3) the rules for compensation for damage caused by a source of increased danger to relations with the use of digital technologies, based on whether the damage caused by the action or inaction of artificial intelligence was predictable.

At the same time, it is also interesting for further research to study the feasibility of introducing into the current legislation rules on compensation for damage caused by artificial intelligence, as a kind of special tort and the use of insurance to minimise the risks of artificial intelligence damage.

REFERENCES

[1] Stefanchuk, M.O. (2020). *Civil legal personality of individuals and features of its implementation*. Kyiv: Artek.

[2] Oxford English and Spanish Dictionary, Thesaurus, and Spanish to English Translator. (2020). Retrived from https://www.lexico.com/definition/artificial_intelligence.

[3] Tyagi, Amit. (2016). Artificial intelligence: boon or bane? *SSRN Electronic Journal*. Retrived from https://www.researchgate.net/publication/307981242_Essay_Artificial_ Intelligence_Boon_or _Bane

[4] Baranov, O.A. (2019). *The internet of things and artificial intelligence: the origins of the problem of legal regulation.* Retrived from http://aphd.ua/publication-376/.

[5] Bernard, M. (2018). Is artificial intelligence dangerous? AI risks everyone should know about. *Forbes*. Retrived from https://www.forbes.com/sites/bernardmarr/2018/11/19/is-artificial-intelligence-dangerous-6-ai-risks-everyone-should-know -about/?sh=1fe0db 724040.
[6] What can artificial intelligence do to the world? (2017). Retrived from https://www.radiosvoboda.org/a/details/28891073.html.
[7] Chen, X., Chen, J., Cheng, G., & Gong, T. (2020) Topics and trends in artificial intelligence assisted human brain research. *PLoS ONE*, 15(4), e0231192. Retrived from https://doi.org/10.1371/journal.pone.0231192.
[8] IEEE Confluence Report on AI and ML Applied to Cybersecurity_9. (2018, April). Retrieved from https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/industry/ieee_confluence_report.pdf.
[9] Hawking, S. (2019). *Black holes and baby universes*. Moscow: AST.
[10] Vyshnovetska, S.V. (2014). *Methodology of labor law science*. Kyiv: Nika-Center.
[11] G20 Ministerial Statement on Trade and Digital Economy. Retrieved from https://www.mofa.go.jp/files/000486596.pdf.
[12] Price II, N.W., & Glenn, C.I. (2019). Privacy in the age of medical big data. *Nature Medicine*, 25, 37-43.
[13] Tomašev, N. (2019). A clinically applicable approach to continuous prediction of future acute kidney injury. *Nature.* 572, 116-119.
[14] Price II, N.W. (2019). Artificial intelligence in the medical system: four roles for potential transformation. *Yale Journal of Law & Technology*, 122, 18.
[15] Aleksiuk, E. (2019). Cyberpunk for lawyers: what you need to know about artificial intelligence. Retrived from https://cedem.org.ua/articles/kiberpank-dlya-yurystiv-shho-potribno-znaty-pro-shtuchnyj-intelekt/.
[16] Čerka, P., Grigienė, J., & Sirbikytė, G. (2017). Is it possible to grant legal personality to artificial intelligence software systems? *Computer Law & Security Review*, 33(5), 685-699. https://doi.org/10.1016/j.clsr.2017.03.022.
[17] McKinsey Global Institute. Jobs lost, jobs gained: What the future of work will mean for jobs, skills, and wages. (2017, November). Retrieved from https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages#.
[18] Hupfer, S. (2020). Getting ahead of the risks of artificial intelligence. *Deloitte Insights*. Retrived from https://www2.deloitte.com/us/en/insights/industry/technology/risks-of-artificial-intelligence.html.
[19] Slayton, R. (2020). The promise and risks of artificial intelligence: a brief history. *War on the Rocks*. Retrived from https://warontherocks.com/2020/06/the-promise-and-risks-of-artificial-intelligence-a-brief-history/.
[20] Firth-Butterfield, K., Madzou, L. (2020). Rethinking risk and compliance for the Age of AI. *World Economic Forum.* Retrived from https://www.weforum.org/agenda/2020/09/rethinking-risk-management-and-compliance-age-of-ai-artificial-intelligence/
[21] Bajorek, J.P. (2019). Voice recognition still has significant race and gender biases. *Harvard Business Review*. Retrived from https://hbr.org/2019/05/voice-recognition-still-has-significant-race-and-gender-biases.

[22] Froomkin, M.A. (2019). When ais outperform doctors: the dangers of a tort-induced over-reliance on machine learning. *Arizona Law Review*, 61, 33.
[23] Vinnyk, O. (2020). Advantages and risks of digitalization of the economy: problems of legal regulation. *Entrepreneurship, Economy and Law,* 3, 56–62.
[24] Ponkin, I.V. & Redkina, A.I. (2018). Artificial intelligence from the point of view of law. *RUDN Journal of Law*, 22(1), 91–109. Retrived from https://www.researchgate.net/publication/324518784_Artificial_Intelligence_from_the_Point_of_View_of_Law.
[25] Artificial intelligence and life in 2030. (2016) One hundred year study on artificial intelligence. Report of the 2015 Study Panel. Retrived from https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai_100_report_0831fnl.pdf.
[26] Scherer, M.U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 29(2), 353-400. Retrived from http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf.
[27] Artificial intelligence: Commission takes forward its work on ethics guidelines. (2019, April). Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1893.
[28] Pozova, D. (2017). The Prospects for the Legal Regulation of Artificial Intelligence Under Eu Legislation. *Časopis Civìlìstiki*, 27, 116–120.
[29] Kostenko, O.V., & Kostenko, V.V. (2020). Legal liability and identification subjects and artificial objects (Ai). *Legal Scientific Electronic Journal,* 1, 158–162.
[30] Kolodin, D., Baytalyuk, D. (2019). To the question of civil liability for the damage caused by robotized mechanisms with artificial intelligence (robots). *Časopis Civìlìstiki*, 33, 87–91.

Maryna M. Velykanova

Doctor of Law, Associate Professor
Associate Professor of the Department of International Relations
Kyiv National University of Culture and Arts
01601, 36 Eugene Konovalets Str., Kyiv, Ukraine

Suggested Citation: Velykanova, M.M. (2020). Artificial intelligence: legal problems and risks. *Journal of the National Academy of Legal Sciences of Ukraine*, 27(4), 185-198.

Submitted: 02/05/2020
Revised: 23/07/2020
Accepted: 09/12/2020