K. S. Zhyhalova,
lawyer, master's degree in law (LL.M. in Law)
Yaroslav Mudryi National Law University

УДК 34.096+347.77+347.78
DOI 10.37749/2308-9636-2021-8(224)-1

PARTICULAR ASPECTS OF THE NECESSITY OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE IN UKRAINE

The purpose of the study was to demonstrate particular legal and objective reasons for necessity and expediency of legal regulation advancement, development and usage of Artificial Intelligence (AI) in Ukraine. Chapter 1 «Understanding of Artificial Intelligence» gives examples of AI applications, doctrinal and diverse legal definitions of AI. Chapter 2 «Necessity and Expediency of legal regulation of Artificial Intelligence in Ukraine» shows the necessity of legal regulation, exemplifies the gaps in current legislation. This Chapter demonstrates that it is paramount to establish protection of IP rights within AI legal relationships in Ukraine. Also, Chapter 2 analyzes particular issues in AI and national, international and social security, questions of data protection. Chapter 3 «Conclusion» demonstrates that absence of specific AI regulation could potentially lead to numerous problems in public/private sectors, for economics, businesses, civilians.

***Key words**: Artificial Intelligence (AI), legal regulation of AI, intellectual property (IP) protection, national security, protection of human rights and freedoms, data protection.*

INTRODUCTION: FORMULATION OF THE PROBLEM

Nowadays practically each of us heard such complex definition as Artificial Intelligence (AI) and it is rapid development all over the World. However, do we actually know, and what is more important, do we understand the definition of AI? It is vital to know how AI works and effects most countries (more specifically Ukraine), economics, public and private sectors, industries, societies and all of us as particular individuals. According to the Pega's (technology company, based in Cambridge, Massachusetts) infographic, from 6,000 consumers only 33 percent admit that they use technology with AI. However, in reality 77 percent of all the respondents are actually use an AI-powered service or device. Moreover, 70 percent think they understand AI, but it does not coincide with reality [1]. Such statistics evidence that many people do not understand the essence of AI and the level of implementation and applicability of AI technologies in our everyday life. Currently, due to the active usage and tremendous growth of AI applications worldwide, many countries (for instance,

EU countries and USA are one of the global leaders in AI field) face legal and practical issues, litigations in AI and other related areas. At the present time, the most important questions of concern are:

1. The level of responsibility for AI technology;

2. Data protection, protection of national security, fundamental human rights and freedoms (during use of AI application);

3. Protection of intellectual property rights on AI components and AI applications/inventions, how AI applications itself could be protected (copyright, patent, trade secret protection);

4. Protection of intellectual property rights of AI developers, engineers, programmers, providers etc.

It is essential to create legislation that could clarify that AI applications should be created and used with adherence rule of law and current legislation. That is why, absence of legal regulation of AI could potentially cause damage national security, fundamental human rights and freedoms. Also, it is hard to foreseen potential violation by AI, without appropriate legal regulation (framework) of AI. Nowadays, crucial issues, connected to AI area are still a part of the debate processes in Ukraine. For Ukraine it is essential to develop Ukrainian AI legal regulation, attract investments, support and encourage IT/AI software developers to provide high quality AI applications in Ukraine. This study demonstrates a concrete examples and cases of international practice in the intellectual property protection, as well as AI and national, international and social security, and data protection. The purpose of the study was to demonstrate particular legal and objective reasons for necessity and expediency of legal regulation advancement, development and usage of AI in Ukraine.

In 2018 Gorshenin Institute in cooperation with Everest group held an opinion poll «Artificial Intelligence: Ukrainian Dimension». The primary sociological data was collected by means of standardized face-to-face interviews (total of 1,000 interviews was conducted (aged 16—65 years old)). According to that sociological study 73.3 percent of respondents answered that they are rather and certainly interested in new technologies, together with 74.1 percent of interviewees answered that they feel the impact of AI in their life. Also, 84.7 percent of respondents heard the term AI, along with 34.8 percent have strong association that AI are robots and robotics [2]. So, what is the definition of AI itself and what is the distinction between AI and robotics?

1. UNDERSTANDING OF ARTIFICIAL INTELLIGENCE

Back in 1995, Russell and Norvig noticed that AI encompasses a huge variety of subfields, from general-purpose areas such as perception and logical reasoning, to specific tasks such as playing chess, proving mathematical theorems, writing poetry, and diagnosing diseases [3, p. 4]. Indeed, present days AI widely used in many industries (for instance, healthcare, education, justice field etc.) by many counties, including Ukraine. The brightest example of usage AI in healthcare area is AI-assisted robotic surgeries [4]. The most famous and widely used AI-assisted robot is the DaVinci surgical system (Intuitive Surgical, Sunnyvale, CA) that can conduct minimally invasive surgeries. The DaVinci is a «master-slave» robot completely dependent upon human control and used worldwide. Despite the fact that the da Vinci robot, first introduced in 2000, and is the predominant commercially available robotic surgery system [5, pp. 1, 3], the first one surgery in Ukraine with the da Vinci was conducted only in 2021 at the Lviv Clinical Emergency Hospital [6]. Noteworthy example of AI in the field of education is worldwide known Ukrainian technology company Grammarly that develops a digital writing tool using AI, which helps to write texts in English [7]. Internet Court of China can be an exemplification in the field of justice. The

«smart court» includes non-human judges, powered by AI and allows participants to register their cases online and resolve their legal cases via a digital court hearing. The Chinese Internet courts handle a variety of disputes, which include intellectual property, e-commerce, financial disputes related to online conduct, loans acquired or performed online, domain name issues, property and civil rights cases involving the Internet, product liability arising from online purchases and certain administrative disputes [8]. In comparison, in Ukraine exists the Electronic Court system (subsystem operates in a test mode) that allows to perform only limited range of actions and only helps to file an exhaustive list of lawsuits, track the progress of the case, file procedural documents, pay court fees and control the receipt of lawsuits against yourself, and all these actions are carried out online [9]. But AI at the Ukrainian Electronic Court system do not make any court decisions on law cases and do not solve any kind of disputes (unlike Internet Court of China, where AI non-human judge resolve certain kind of cases and adjudicate).

Important to emphasize that in the field of AI there is a differentiation of AI applications (systems). In 1980 John R. Searle [10] (University of California, Berkeley) distinguish «strong» AI from the «weak» AI (also called «narrow» AI). According to the recent white paper «Artificial Intelligence and Robotics» (2018) most existing intelligent systems that use machine learning, pattern recognition, data mining or natural language processing are examples of «weak» AI. Intelligent systems, powered with «weak» AI include recommender systems, spam filters, self-driving cars, and industrial robots. In contrast, «strong» AI is usually described as an intelligent system endowed with real consciousness and is able to think and reason in the same way as a human being [11, p. 6]. Enrique Piracйs stated that «strong» AI generally refers to the ability of a machine to perform «general intelligent action», which is why it is also referred to as artificial general intelligence [12, p. 297]. In addition, any kind of AI («weak» AI, nor «strong» AI) is not equal to the term robotics. Talking about distinctions between AI and Robotics, Robots are programmable machines that can carry out routine tasks semi-or-fully autonomously. Artificial intelligence, on the other hand, is the development of computer models to complete tasks that would otherwise require human intelligence. In other words, artificial intelligence algorithms are generally self-trained to carry out tasks with some level of human behavior (e. g. language understanding capabilities). This shows that the two branches are fundamentally different, in that robots carry out pre-defined and routine tasks while artificial intelligence attempts to mimic «intelligence». There is, however, an intersection of these two branches, which is artificially intelligent machines. Artificially intelligent robots or machines are the bridge between artificial intelligence and robotics [13, p. 1].

Thus, AI and Robotic are completely separate fields of technology. Both, there are complex and have their own individual characteristics, elements, components and essence. However, AI and Robots areas correlate and complement each other meanwhile creating and performing particular tasks. In Robotics field there are different types of robots (less or more advanced). There are some key features for understanding of main differences between AI and Robots (especially advanced artificial intelligent Robots). AI is an intelligent algorithm that is an intangible asset, while Robotics (Robots) have physical form of expression. In simple terms, AI as an intangible algorithm (roughly speaking could be compared to simulation of human brain activity) is one of the general components of such type of robots as advanced intelligent Robots that are tangible objects, which again, roughly speaking, could be compared to physical body (objects).

Fast inevitable advancement and spread of AI (regardless of the AI country of origin) to all countries, economics, public and/or private sectors necessitate development and adoption of law that could regulate the advancement, development and usage of AI (especially in Ukraine) with the strong purpose to:

a) protect national security;

b) fundamental human rights and freedoms (for instance, the right to human dignity (according to Article 1 of the Charter of Fundamental Rights of the European Union [14], Convention for the Protection of Human Rights and Fundamental Freedoms [15], Protocol No. 13 to the Convention for the Protection of Human Rights and Fundamental Freedoms concerning the abolition of the death penalty in all circumstances [16]), respect for private life (Article 7 of the Charter of Fundamental Rights of the European Union, Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms), protection of personal data (Article 8 of the Charter of Fundamental Rights of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council 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 [17]), the right to protection of intellectual property (Article 17(2) of the Charter of Fundamental Rights of the European Union, Berne Convention for the Protection of Literary and Artistic Works [18], Paris Convention for the Protection of Industrial Property [19]), freedom of art and science (Article 13 of the Charter of Fundamental Rights of the European Union);

c) to encourage IT and AI software developers, engineers, representatives to work on and to create high quality AI applications with adherence rule of law.

Importantly, legal regulation of AI will create conducive space for AI development and as a result will cause economic and business growth. That regulation should start from giving legal definition of AI. There are a wide range of diverse terminology of AI. The doctrinal AI definition is not cutting-edge. The first «AI period» began with the Dartmouth conference in 1956, where AI got its name and mission. McCarthy coined the term «Artificial Intelligence» (AI), which became the name of the scientific field [20, p. 7]. AI is a young discipline of sixty years, which is a set of sciences, theories and techniques (including mathematical logic, statistics, probabilities, computational neurobiology, computer science) that aims to imitate the cognitive abilities of a human being [21].

Currently, term AI has no single consolidated legal definition. For instance, World Intellectual Property Organization (WIPO) do not give precise and clear legal expression of AI. On the WIPO web-site stated that AI is generally considered to be a discipline of computer science that is aimed at developing machines and systems that can carry out tasks considered to require human intelligence [22]. On Third Session of the «WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI)» was concurred and said a basic definition of AI and AI-related terms needs to be agreed upon. However, it was also generally recognized that establishing a definition would be difficult given how fast AI technologies are evolving [23, para. 16]. In contrast, Organisation for Economic Co-operation and Development (OECD) gives definition to AI system that is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments [24]. The Council of Europe Ad hoc Committee on Artificial Intelligence (CAHAI) in the official Glossary gives the term AI as a set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being [25]. In addition, the European Union's institutions that are responsible for the development of legislation in AI field in

AI initiatives give proposals on AI matters, discuss the most concrete and accurate term of AI by giving definition of AI as AI systems. According to the Policy paper of European Commission «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» AI refers to systems that display intelligent behaviour by analysing their environment and taking actions — with some degree of autonomy — to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e. g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e. g. advanced robots, autonomous cars, drones or Internet of Things applications) [26, p. 1]. In any new legal instrument, the definition of AI will need to be sufficiently flexible to accommodate technical progress while being precise enough to provide the necessary legal certainty [27, p. 16]. In the proposal for a Regulation of the European Parliament and of the Council «Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts» from 2021/0106 (COD) [28], stated that «artificial intelligence system» (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with» (Article 3 (1) of Regulation). Also, mentioned Proposal suggested that the definition of AI system should be based on the key functional characteristics of the software, in particular the ability, for a given set of human-defined objectives, to generate outputs such as content, predictions, recommendations, or decisions which influence the environment with which the system interacts, be it in a physical or digital dimension. The definition of AI system should be complemented by a list of specific techniques and approaches used for its development, which should be kept up-to-date in the light of market and technological developments through the adoption of delegated acts by the Commission to amend that list ((6) of Regulation). Moreover, The European Commission appointed a group of experts to provide advice on artificial intelligence strategy. High-level expert group on artificial intelligence (AI HLEG) in a document «A definition of AI: Main capabilities and scientific disciplines» gives propose to update AI definition and delimitate AI as a system and AI as a scientific discipline. According to this document, AI refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems) [29, p. 7].

The first country that on legislation level enacted term AI is the United States of America (USA). The definition of AI was codified in statute John S. McCain National Defense Authorization Act for Fiscal Year 2019 in section 238 (g), where the AI term includes the following — any artificial system that performs tasks

under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. An artificial system designed to think or act like a human, including cognitive architectures and neural networks. A set of techniques, including machine learning, that is designed to approximate a cognitive task. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting [30].

2. NECESSITY AND EXPEDIENCY OF LEGAL REGULATION OF ARTIFICIAL INTELLIGENCE IN UKRAINE

Eastern Europe is taking the lead in offshore software development and Ukraine is the hottest outsourcing destination in the region. Ukraine is on its way to becoming a global tech powerhouse, taking 11th place on the list of the top offshore software development countries in the world (as of 2020) [31]. According to the Government AI Readiness Index 2020, Ukraine has the largest number of AI and machine learning providers in the Eastern Europe region [32, p. 59].

Tremendous growth of Artificial Intelligence all over the world raised crucial issues, connected to that area. On January 2020, Ministry and Committee of Digital Transformation formed an Expert Committee on the Development of Artificial Intelligence. Also, Ukraine is a country-member of the Ad Hoc Committee on Artificial Intelligence (CAHAI) of the Council of Europe [33]. Moreover, in 2019 Ukraine as a non-member of OECD (Organization for Economic Co-operation and Development) become a country adherent to the Artificial Intelligence Principles (OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449). Additionally, Ukraine is observing member of Standardization in the area of Artificial Intelligence (ISO/IEC JTC 1/SC 42 Artificial intelligence) [34]. In December 2020 the Cabinet of Ministers of Ukraine approved «The Concept for the Development of Artificial Intelligence in Ukraine» [35]. This Concept covers no more than definition of AI and further directions of the AI activity in the corresponding branches in Ukraine. However, Ukraine still remains in the process of discussing and creating of the legal regulation of basic approaches of development and usage of AI. It is essential to promote public and academic discussions, organize publicly available conversations on AI matters with strong purpose to fill the gaps in current Ukrainian legislation and to foster appropriate understanding and interpretation of AI definitions. Also, take into consideration international approaches of legal AI regulation as well as international case law on AI matters. What is more, it is highly crucial to draw information from national and international resources, observe, filter and critically analyze international approaches of AI legal regulations (Policies, Principles, Templates etc.) as well as explore international protection practices, which are widely exist in most developed countries. So, why it is important to develop and implement an effective legal regulation of development and usage of AI in Ukraine?

I. First of all, there are a numerous number of questions that seek for a legal regulation in the intellectual property protection aspects. There are four potential answers to this question of ownership, that stem from breaking down the machine learning pipeline into its parts: input (the training data that goes into the model), the model itself (a process of iterating and evaluating over results until a sufficient success threshold is reached), and finally the tangible output of a model which can take the form of a

generated art piece, story, etc. From this, a list of potential intellectual property owners becomes: the creator of the training data, the AI model itself, the programmer who curates the system, and lastly no one at all if if it determined that AI-generated work are unprotectable and should become public domain. In addition to thinking about this concept of assigned ownership as a designation to the individual (or algorithm) with the greatest role in the resulting creative output, the problem of assignment needs to also uphold the greater roles of intellectual property law as described by intellectual property law theory [36]. One of the main problems that should be regulated is establishment of effective mechanism of protection of intellectual property rights within AI legal relationships in Ukraine, e. g., in the following aspects:

1. Contractual protection of intellectual property rights of AI developers, engineers, programmers, providers.

There are, at least, two types of relationships: 1) between AI developers/ providers and users and 2) between AI developers and their employers. Generally stated that the inventor is the first owner of any patent which is applied for and granted over that invention. AI cannot be the inventor (and therefore the owner of a patent) because «devising» an invention is a human activity which involves contributing to the inventive concept. The invention and any patent granted over it will, as a consequence, belong either to the human deviser or, if an employee, their employer. In relation to copyright law, there is a scale with, at one end, AI being used as a tool, admittedly a very sophisticated tool, to help develop new inventions [37]. In the research «Expert Q&A on Artificial Intelligence (AI) Licensing» for purposes of this discussion, the term «provider» refers to the AI licensor and the term «user» refers to the business that is the AI licensee. The provider (AI licensor) typically is the owner of the AI solution and provides a license to the AI solution to the user. The license may include restrictions on use, such as a field of use restriction, territorial limitations, or uses prohibited for risk, legal, or ethical reasons. For example, voice recognition technology may be appropriate for helping customers to navigate a voice response unit but may not be appropriate for analysis to impute IQ scores to prescreen for employment or confer other benefits. Since US IP laws do not squarely cover AI, as between an AI provider and user, contractual terms are the best way to attempt to gain the benefits of IP protections in AI license agreements. For instance, the parties could:

a) designate certain AI components as trade secrets;

b) protect AI components by: limiting use rights; designating AI components as confidential information in the terms and conditions; and restricting use of confidential information. Include assignment rights in AI evolutions from one party or the other;

c) determine the license and use rights the parties want to establish between the provider and the user for each AI component;

d) clearly articulate the rights in the terms and conditions [38, pp. 3, 4].

Depending on the AI arrangement, the provider may provide a license to software or grant access to cloud services containing the AI. References to AI licensing, therefore, typically include: 1. On-premises licenses of AI, where the user installs, trains, and operates the AI solution; 2. Subscription to software as a service (SaaS) or other cloud services the provider offers where the user accesses the AI solution in the cloud via the internet, and the provider often trains the AI solution. For more on software licensing, SaaS, and other cloud services: 1. Software License Agreements; 2. Software as a Service (SaaS) Agreements; 3. Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) Agreements [38, pp. 1, 3, 4].

Thousands of researchers and engineers are currently working on machine learning (ML) and AI software. However, developers often have limited or even no control over how this software is used once

it is released publicly. For instance, the same AI tool that can be used for faster and more accurate cancer diagnoses can also be used in powerful surveillance systems. This lack of control is especially salient when a developer is working on open-source ML or AI software packages, which are foundational to a wide variety of the most beneficial ML and AI applications. Responsible AI Licenses (RAIL) empower developers to restrict the use of their AI technology in order to prevent irresponsible and harmful applications [39]. Both a source code license [40] and an end-user license [41] developers can include with AI software to restrict its use. Licensees should consider contractual ownership and use of the components of AI, including the AI tool, evolutionary changes to the AI tool, the training data and instructions, and the output of operation of the AI tool. When licensing AI, AI providers expect to continue to own the underlying AI tool, and some may expect to own the evolutionary changes as well. Much of the AI that businesses will use may require training. The license should address which party will train the AI, which party will own the training instructions and which party will own the evolution of the AI tool based on the training [42]. As we have seen, contracts play a major role in securing and assigning IP rights in the development of AI technology. Furthermore, contracts help fill gaps and protect training datasets, and AI generated outputs that are not protectable by IP. It is therefore important for companies to have contracts that define in detail the scope of protection, and how these elements can be used. Well-drafted agreements ensure a successful business relationship, and avoid costly litigation [43, p. 18].

2. Protection of intellectual property rights on AI components and AI applications/inventions itself (not result of work that AI created)

Patents, copyright and trade secrets are all viable means of protecting AI technology. However, the right approach is dependent on many factors including: the type of AI to be protected; the likely lifespan of the technology; the value of the AI; and its importance to the business [44]. Corporate AI developers face two key decisions around how to protect their AI-related intellectual property: whether or not to patent AI techniques and systems, and whether to open-source models or keep them private as trade secrets. A prevalent strategy among top AI developers today involves accumulating patents while simultaneously sharing research with the open-source community. For example, Microsoft holds the most number of machine learning patents in the US,but is also an active participant in the open-source community. Amazon, Google, IBM, Facebook, Baidu, Tencent, and several other companies are prolific patent holders in AI while also open-sourcing substantial portions of their systems and sharing their work at academic conferences [45, p. 2]. AI technology may be suited to trade secret protection. It is often the case that the most competitively valuable information in a computer implemented product is the algorithm. Consumers of the product interact only with the AI interface and will typically not have access to the algorithm. This means the algorithm could be protected as a trade secret provided the appropriate security measures were in place. In fact, Google's search algorithm is a famous trade secret. The key advantage that trade secret protection provides over patents and copyright is that trade secrets can protect a broader range of information (including business methods, inventions, and even original ideas in certain circumstances) on the condition that the information is kept secret. However, trade secret protection can be instantaneously and irreversibly lost if the secret is disclosed publicly. And even if the trade secret remains in place, the secret holder has no recourse if a competitor independently develops the same AI technology that is protected by the secret [44].

3. Copyright protection of AI/AI-generated objects, outputs

Andres Guadamuz (University of Sussex, United Kingdom) stated that creating works using AI could have very important implications for copyright law. Traditionally, the ownership of copyright in computer-generated works was not in question because the program was merely a tool that supported the creative process, very much like a pen and paper. AI is already being used to generate works in music, journalism and gaming. These works could in theory be deemed free of copyright because they are not created by a human author. As such, they could be freely used and reused by anyone. That would be very bad news for the companies selling the works. Imagine you invest millions in a system that generates music for video games, only to find that the music is not protected by law and can be used without payment by anyone in the world [46]. Important to mention that AI created art has been exhibited in many top contemporary art galleries in London, New York City, and around the world. In addition, a single AI generated painting sold for nearly half a million dollars at Christie's auction house, which is strong evidence supporting the financial value — and historical significance — of AI generated art [47]. In October 2018, a work of art by Edmond de Belamie, which was created with the help of an intelligent algorithm, was auctioned for $432,500 at Christie's Auction House [48].

4. Patent protection (patentability) of AI/AI related objects; issues in inventorship and ownership of AI, e. g., who could be considered as inventor — AI itself or natural person (individual/ individuals collectively), who took no involvement in the invention process, if the invention itself was autonomously generated by AI.

Ryan Abbott (University of Surrey, UK; UCLA, California, USA) believes that patents can promote disclosure of information and the commercialization of socially valuable products. Patents for AI-generated works will accomplish these goals as well as any other patents. By contrast, failing to allow protection for inventions generated by AI would mean that, in the future, businesses may not be able to use AI to invent, even when it becomes more effective than people in solving certain problems. Such a scenario would also encourage gamesmanship with patent offices by failing to declare a filing is based on an AI-generated invention [49]. Lastly, the fact that a human finances, owns, or operates AI is insufficient to qualify that person as an inventor. As made clear in TS Holdings, financing or initiating the process of invention (e.g., by setting inventors to task) does not satisfy the standard to be named on a patent. In such situations, a person may be responsible for an invention, but they have not actually invented a new technology [50, p. 1963]. Many AI companies are pursuing what may seem like a counterintuitive IP strategy: aggressively patenting AI technologies while sharing them freely. They experience competitive pressure to patent in order to present the threat of a countersuit if another company sues them for IP infringement [45].

Currently, it seems to be really hard to obtain a patent on AI/AI-related applications, especially when they are generated by computer systems. For instance, famous Alice Corporation Pty. Ltd. v. CLS Bank International et al. case (Alice case, 2014) and other cases (which often, afterwards, were based and decided on the Alice case argumentation) in the United States common law system are demonstrate that software-related inventions and, what is more, AI-generated application, frequently considered to be not patent-eligible. In the Alice case petitioner — Alice Corporation is the assignee of several patents that disclose schemes to manage certain forms of financial risk. The patents at issue in this case disclose a computer-implemented scheme for mitigating «settlement risk» (i. e., the risk that only one party to a financial transaction will pay what it owes) by using a third-party intermediary. The invention «enables the management of risk relating to specified, yet unknown,

future events», «invention relates to methods and apparatus, including electrical computers and data processing systems applied to financial matters and risk management». The court decided that the claims at issue are drawn to the abstract idea of intermediated settlement, and that merely requiring generic computer implementation fails to transform that abstract idea into a patent-eligible invention. Also, was concluded that petitioner's claims «draw on the abstract idea of reducing settlement risk by effecting trades through a third-party intermediary», and that the use of a computer to maintain, adjust, and reconcile shadow accounts added nothing of substance to that abstract idea. The «abstract ideas» category embodies «the longstanding rule that '[a]n idea of itself is not patentable'». The Supreme Court of the United States concluded that the method claims, which merely require generic computer implementation, fail to transform that abstract idea into a patent-eligible invention and «held that simply implementing a mathematical principle on a physical machine, namely a computer, is not a patentable application of that principle» [51]. In the PurePredictive, Inc. v. H2O. AI, Inc. case (2017), plaintiff — PurePredictive, Inc is the technology company that uses artificial intelligence to provide insight into business's data through the use of predictive modeling and owner of the '446 Patent. United States District Court, N.D. California used Alice argumentation (among other cases) to find the '446 patent «an automated factory for predictive analytics» as patent ineligible, because claims are directed to the abstract concept of the manipulation of mathematical functions and make use of computers only as tools, rather than provide a specific improvement on a computer-related technology [52]. All above mentioned and a few similar cases (particularly like in the Alice and Pure Predictive cases) demonstrate that previously patented software/AI-generated inventions can be found patent-ineligible by filing a lawsuit or counterclaim for infringement by competitors. In point of fact, financial and intellectual investments and efforts particular individuals or companies could be depreciated. From the above mentioned, it may follow that disregard for the existence of a patent and infringements in Intellectual Property field take place, due to the uncertainties, absence or lack of AI Ethics, Principles, legal provisions in AI field.

Nowadays, it is generally established that AI application cannot be registered as inventor. An American artificial intelligence expert, Stephen Thaler, developed AI system «DABUS» that invented two technical solutions involving food containers and light for attracting enhanced attention. Since 2018, Thaler had filed applications in various countries and would like to designate the AI system «DABUS» instead of himself as the inventor. This is the first time, where AI had been designated as the inventor in an application. However, the above applications were rejected by patent offices in multiple countries because of AI inventor issues [53]. The United States Patent and Trademark Office (USPTO) in Decision on Petition stated that it is axiomatic that inventors are the individuals that conceive of the invention. According to the 35 U.S. Code § 100(f) the term «inventor» means the individual or, if a joint invention, the individuals collectively who invented or discovered the subject matter of the invention. When explaining the distinction between inventorship and ownership of an invention by a corporation, the Federal Circuit in an earlier decision, Beech Aircraft Corp. v. EDO Corp., stated that: «only natural persons can be «inventors». So, U.S patent law does not permit a machine to be named as the inventor in a patent application [54]. The European Patent Office (EPO) in Decision also refused to recognize AI as inventor. So, the applicant Stephen Thaler is still in appeals process against decision and intends to register «DABUS» as the inventor [55]. The UK Intellectual

Property Office (UKIPO) in the Decision stated that DABUS is not a person as envisaged by sections 7 and 13 of the UK Patent Act 1977 and cannot be considered an inventor. What is more, in the Conclusion of the Decision was stated that even «if I am wrong on this point, the applicant is still not entitled to apply for a patent simply by virtue of ownership of DABUS, because a satisfactory derivation of right has not been provided» [56].

II. AI and national, international and social security, and data protection are another vulnerable and widely discussed aspects that needed for the legal regulation AI and national security, as well as data protection are huge and extremely essential areas that must be carefully and responsibly discussed during creation of AI regulation policy in Ukraine. These fields are broad, have own advantages and disadvantages and include many aspects that needed sufficient legal provisions, which would protect national security, prevent data breach on all kind of levels. But at the same time Ukrainian government may encourage to develop and invest in AI area, with the purpose for the technological progress for the common good.

There are a number of direct applications of AI relevant for national security purposes [57, p. 3]. Important to mention that these AI applications could have one country of origin and, at the same time, could potentially cause damage on national and/or international levels, economics, businesses, and not excluding, of causing damages to other countries. This fact proves that legal regulation of AI should be one the main priorities in each country that has purpose to develop effective AI Policy.

Talking about disadvantages, unlike traditional cyberattacks that are caused by «bugs» or human mistakes in code, AI attacks are enabled by inherent limitations in the underlying AI algorithms that currently cannot be fixed. Further, AI attacks fundamentally expand the set of entities that can be used to execute cyberattacks. For the first time, physical objects can be now used for cyberattacks (e. g., an AI attack can transform a stop sign into a green light in the eyes of a self-driving car by simply placing a few pieces of tape on the stop sign itself). Data can also be weaponized in new ways using these attacks, requiring changes in the way data is collected, stored, and used. There are five areas most immediately affected by artificial intelligence attacks: content filters, the military, law enforcement, traditionally human-based tasks being replaced by AI, and civil society. These areas are attractive targets for attack, and are growing more vulnerable due to their increasing adoption of artificial intelligence for critical tasks [58]. AI is being incorporated into a number of other intelligences, surveillance, and reconnaissance applications, as well as in logistics, cyberspace operations, information operations, command and control, semiautonomous and autonomous vehicles, and lethal autonomous weapon systems [59, p. 10]. Proliferation of AI in weapon systems in combination with absence of international regulation on their development could lead to a new trilateral Arms race [60, p. 4]. Many major cybersecurity failures began with «social engineering», wherein the attacker manipulates a user into compromising their own security. Email phishing to trick users into revealing their passwords is a well-known example. The most effective phishing attacks are human-customized to target the specific victim (aka spear-phishing attacks) — for instance, by impersonating their coworkers, family members, or specific online services that they use. AI technology offers the potential to automate this target customization, matching targeting data to the phishing message and thereby increasing the effectiveness of social engineering attacks. Moreover, AI systems with the ability to create realistic, low-cost audio and video forgeries (discussed more below) will expand the phishing attack space from email to other communication domains, such as phone

calls and video conferencing. Another bright example, when AI systems able to recognize patterns and calculate the probability of future events, when applied to human behavior analysis, can reinforce echo chambers and confirmation bias. Machine learning algorithms on social media platforms prioritize content that users are already expected to favor and produce messages targeted at those already susceptible to them. [57, pp. 4, 5].

Interesting fact that in 2019 plaintiffs Cyrus A. Parsa, the Al Organization, Inc. and others filed a lawsuit against defendants Google L.L.C, Facebook Inc, DeepMind Inc. and others, with 26 complaints to the United States District Court Southern District of California. Main plaintiffs' claims are misuse of AI, cybernetics, robotics, biometrics, bioengineering, 5G and quantum computing technology, endangering the human race with the misuse of AI technology, transfer of AI weapon technology to China, bio-digital social programming of the human race by use of their biometrics and AI and other complaints [61]. Currently, the decision or comments on this case have not been made publicly availably (if any existing).

However, talking about advantages, AI is useful in particular with respect to Human resources and manning requirements: making (heterogeneous) systems work together; data exchange; command coordination; target allocation (also between nations); working with fewer resources; taking the man on/over the loop; coordination of sensors and effectors; threat detection and identification; semi-autonomous weapon allocation; improving timeliness (fast threat, pop up, numerous threat); derivation of intent, situational awareness and evaluation. The main applications of Artificial Intelligence and Machine Learning are to enhance C2, Communications, Sensors, Integration and Interoperability [62, p. 76]. The maturation of the Information Age has forced some adaptation and evolution in our laws, regulations, and policies. But the pace and intensity of technological change has often made it difficult for the policy, regulations, and laws to keep up. As has been the case in other periods of intense change, the lag in the evolution of laws and regulations can lead to significant policy gaps. The legal standards of reasonable or acceptable privacy need renegotiation to accommodate new technologies that are being adopted at pace and scale [63, p. 2].

In executive summary of Study of Belfer Center for Science and International Affairs Harvard Kennedy School was clarified main current realities such as: researchers in the field of AI have demonstrated significant technical progress over the past five years, much faster than was previously anticipated; most AI research advances are occurring in the private sector and academia; existing capabilities in AI have significant potential for national security; future progress in AI has the potential to be a transformative national security technology, on a par with nuclear weapons, aircraft, computers, and biotech; advances in AI will affect national security by driving change in three areas: military superiority, information superiority, and economic superiority [64].

In a world in which algorithms reign, the research talent and resources to develop those algorithms become preeminent. Current supply of this talent cannot meet global demand. As a result, policymakers at the national level must find ways to attract foreign talent to their country, to retain the talent that does come, and to develop new talent. The resulting policy levers are things like visa controls, industrial strategies, worker retraining and certification frameworks for AI skills, and educational investments to meet AI faculty and teacher shortages. Given the centrality of AI talent for algorithmic advances, these routine government functions can take on significant national security and economic implications. Though seemingly mundane, this ground is the terrain on which geopolitical competition in the age of AI is

first fought. Privacy issues rise in importance the more data matters for AI. Insofar as tension exists between the privacy rights of users and the value of their data in training machine learning systems, governments must manage the balance. They will have to craft privacy laws and regulations that protect the civil liberties and rights of individuals without unduly constraining the innovation that using their data for training might enable [65, p. 11, 12].

CONCLUSION

Development and everyday usage of AI applications is an inevitable process, in our digital age. Progress in IT and AI areas is unstoppable and develops more and more every day. Unfortunately, countries, which do not properly develop the conducive AI ecosystem, do not make any investments, do not create AI legislation and do not stimulate young and proficient IT/AI developers. It is potentially leads:

a) to become vulnerable to cyberattacks on public and private levels, or on politicians;

b) data breach could appear;

c) economics and businesses could lose financial benefits and profit;

d) absence of own strong AI base and Policy in the country, may cause to become completely defendant on World's Global AI leaders and their decisions etc.

Hopefully, this story is not about Ukraine. Without any doubts, there are a several crucial issues that have to be legally clarified in Ukrainian legislation. Numerous gaps in AI and Intellectual Property fields, absence of specialized AI legislation, necessity of strengthening of data protection field, protection of national security, fundamental human rights, strengthening copyright, patent protection of AI/AI outputs should be priority of Ukrainian public policy makers. Ukraine right now is on it is way to foster advancement of IT and AI markets. There are a number of successful Ukrainian AI applications. Such as: 1) Ukrainian technology company Grammarly that develops a digital writing tool using AI, which helps to write texts in English; 2) Agrolabs is utilizing IoT (internet of things), robotics and AI to help farmers achieve a full control over the growing process; 3) Agrieye develops a drone packed with sensors and multispectral camera that uses remote sensing, unmanned air vehicles, and big and open data analyses; 4) Chatbots.Studio is dedicated focus on business automation and AI chatbots development, their bots already serve in banks, insurance, telecoms, retail and service companies; 5) Court on the Palm (Суд на долоні) is analytical tool for searching court decisions in a faster way) etc.

However, AI leading countries such as the United States of America (USA), China and EU still have much broader AI markets and experience, huge competition that attract many Ukrainians. That is why, it is not surprise that intelligent Ukrainian IT/AI developers leave motherland looking for a better career perspective, assurance in protection of their rights, financial bonuses and stability. For a number of reasons, it is extremely important to deeply research and analyze of the USA (despite the fact that the USA is a common law system), European Union (EU) AI policies, WIPO White Papers and Recommendations, International and National researches. Firstly, for Ukraine it is paramount to follow and to take an active part in discussions on AI topics dedicated to the legal regulation on AI that currently held worldwide (especially when they are held in the virtual format). Secondly, Ukrainian legislators may find many progressive views and ideas that could help to create and afterwards, implement the most accurate AI legal provisions in Ukraine by exploring the diverse world's practice and by analyzing different visions on similar AI problems that are exist in Ukraine. Creation of legal regulation of advancement, development and usage of AI could attract and stimulate IT/AI progress, and would promote adherence and trust in our legislation system. What is more, lack of clarity and general understanding around AI in

Ukrainian society could lead to descension of involvement, understanding and interest on AI matters. Due to the fact that Ukraine already develops some great AI applications in many industries, without appropriate legislation might be hard to prove and define, for instance, the level of responsibility for possible violation by this AI application. General AI provisions needed to be established in order to understand, who is liable and responsible for the violation that was made by AI (who is liable, kind of infringement, level of responsibility). In the case of violation of privacy right/data breach by AI application of individual/particular group of people, who will be responsible — AI application itself, individual/group of individuals, who created and developed AI software (AI developers, engineers etc.) or AI developer's employer. Also, it could be great to create field-specific agency or non-profit organization (public or private), where IT/AI engineers along with legal professionals could directly give legal aid, consultations, deal and assist with such specific AI cases. Also, highly essential to foreseen potential violations of national security, fundamental human rights from the AI perspective. Legislation on AI and IP matters also should be on agenda. It is essential to emphasize on necessity of raising legal academic discussions, legislative initiatives, dedicated to the legal regulation of AI in Ukraine. It is important purpose to develop and foster creation of AI legal regulation, further advancement of AI legislation, as well as establishment of effective mechanism of protection of Intellectual Property and Technology rights in Ukraine.

At the same time, it is vital to let and encourage AI bring social and economic benefits to the country, economics, civilians and businesses. By encouragement of AI area could be implied reinforcement of IT/AI engineers, developers and other related positions to that area. For instance:

a) support and encourage of Ukrainian software developers, AI engineers, IT representatives to work on and to create more and more Ukrainian AI applications in Ukraine;

b) attract investments and investors for financial incentives in AI area;

c) arrange no-charge international AI career enhancement trainings for experience shearing, which will help to expand professional opportunities;

d) organize no charge workshops, forums, national and international conferences, discussions together with international organizations that would be dedicated to the AI matters. That would give an opportunity to receive up-to-date information and share bilateral knowledge, examine and deepen AI experience for all the participants.

Currently, Ukraine is in the progress of AI development. And to become a global leader in AI in healthcare, agriculture, education, justice, banking and financial services, logistics industries, Ukraine shall make efforts to create a legal framework to wit template of principles, ethics, particular provisions of legal regulation of advancement, development and usage AI in Ukraine. In this research were used general scientific and special scientific methods such as formal-logical, comparative, dialectical, normative, systemic, analysis, synthesis, induction and deduction, the method of comparison.

References

1. Pega. (2019). What Consumers Really Think About AI [Infographic]. Pega.com. Last accessed 23 Sept. 2021. URL: https://www.pega.com/system/files/resources/2019-03/what-consumers-really-think-of-ai-infographic.pdf?_rid=YToxOntzOjc6ImNvbnRfaWQiO3M6OToiQ09OVC02MzMyIjt9.

2. Gorshenin Institute in cooperation, Everest innovation integrator. (2018). Artificial Intelligence: Ukrainian Dimension [Infographic, Opinion poll findings in Microsoft PowerPoint slides]. Gorshenin.ua. Last accessed 23 Sept. 2021. URL: http://gorshenin.ua/publication/shtuchnij-intelekt-ukrayinskij-vimir/.

3. Russell S. J. and Norvig P. (1995). Artificial Intelligence: A Modern Approach. Prentice Hall, Englewood Cliffs, New Jersey 07632. Last accessed 23 Sept. 2021. URL: https://www.cin.ufpe.br/~tfl2/artificial-intelligence-modern-approach.9780131038059.25368.pdf.

4. Marr, B. (2018, July 27). How Is AI Used In Healthcare - 5 Powerful Real-World Examples That Show The Latest Advances. Forbes. Last accessed 23 Sept. 2021. URL: https://www.forbes.com/sites/bernardmarr/2018/07/27/how-is-ai-used-in-healthcare-5-powerful-real-world-examples-that-show-the-latest-advances/?sh=2010d7ff5dfb.

5. Panesar, S., Fernandez-Miranda, J., Kliot, M., Cagle, Y., Chander, D., & Morey, J. (2019). Artificial Intelligence and the Future of Surgical Robotics. Annals of Surgery, Volume XX, Number XX, 1—4. Last accessed 23 Sept. 2021. URL: https://www.researchgate.net/publication/331959548_Artificial_Intelligence_and_the_Future_of_Surgical_Robotics.

6. Lutsenko, E. (2021, March 1). For the first time, in Ukraine (Lviv) surgery was conducted with the DaVinci robot surgical system. Hromadske. Last accessed 23 Sept. 2021. URL: https://hromadske.ua/ru/posts/vo-lvove-robot-hirurg-da-vinci-vpervye-v-ukraine-prooperirovalrebenka.

7. Yarova, M. (2019, October 10). Ukrainian Grammarly raises $90M at a valuation of $1B and becomes a unicorn. Ain.ua. Last accessed 23 Sept. 2021. URL: https://ain.ua/en/2019/10/10/grammarly-raises-90m-and-becomes-a-unicorn/.

8. Vasdani, T. (2020, February). Robot justice: China's use of Internet courts. LexisNexis. Last accessed 23 Sept. 2021. URL: https://www.lexisnexis.ca/en-ca/ihc/2020-02/robot-justice-chinas-use-of-internet-courts.page.

9. Shemshuchenko, V. (2020, January 29). Artificial intelligence in justice field. Cedem.org.ua. Last accessed 23 Sept. 2021. URL: https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/.

10. Searle, J. R. (1980). Minds, brains, and programs. The behavioral and brain sciences. 3, 417—457. Cambridge University Press. Last accessed 23 Sept. 2021. URL: https://www.law.upenn.edu/live/files/3413-searle-j-minds-brains-and-programs-1980pdf.

11. Perez, J. A., Deligianni, F., Ravi, D. & Yang, G-Z (2018). Artificial Intelligence and Robotics. eBook Edition: 2018, Copyrighted from UKRAS.Org. Last accessed 23 Sept. 2021. URL: https://arxiv.org/ftp/arxiv/papers/1803/1803.10813.pdf.

12. Piracйs, E. (2018). The Future of Human Rights Technology. Cambridge University Press. 289—308. Last accessed 23 Sept. 2021. URL: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/FDEA9B9760BB34F94BA47BA8148A6F11/9781107179639c13_289—308.pdf/future_of_human_rights_technology.pdf.

13. Global Information Service. (2020). Accessing Artificial Intelligence & Robotics: Nasdaq CTA Artificial Intelligence & Robotics Index — Spring 2020 (NQROBO). Last accessed 23 Sept. 2021. URL: https://indexes.nasdaqomx.com/docs/NQROBO%20Research.pdf.

14. Charter of Fundamental Rights of the European Union, Document 12012P/TXT, Official Journal of the European Union. Last accessed 23 Sept. 2021. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT.

15. Convention for the Protection of Human Rights and Fundamental Freedoms. Rome, 4.XI.1950. 5-32. Last accessed 23 Sept. 2021. URL: https://www.echr.coe.int/Documents/Convention_ENG.pdf.

16. Protocol No. 13 to the Convention for the Protection of Human Rights and Fundamental Freedoms concerning the abolition of the death penalty in all circumstances. Vilnius, 3.V. 2002. 54—57. Last accessed 23 Sept. 2021. URL: https://www.echr.coe.int/Documents/Convention_ENG.pdf.

17. Regulation (EU) 2016/679 of the European Parliament and of the 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) (Text with EEA relevance). Document 02016R0679-20160504. 04.05.2016. Last accessed 23 Sept. 2021. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:02016R0679-20160504.

18. Berne Convention for the Protection of Literary and Artistic Works. Paris Act of July 24, 1971, as amended on September 28, 1979. Last accessed 23 Sept. 2021. URL: https://www.wipo.int/edocs/lexdocs/treaties/en/berne/trt_berne_001en.pdf.

19. Paris Convention for the Protection of Industrial Property of March 20, 1883. Last accessed 23 Sept. 2021. URL: https://www.wipo.int/edocs/lexdocs/treaties/en/paris/trt_paris_001en.pdf.

20. Delipetrev, B., Tsinarakii, C., Kostiж, U. «AI Watch: Historical Evolution of Artificial Intelligence». EUR 30221EN, Publications Office of the European Union. Luxembourg. 2020. Doi: 10.2760/801580, JRC120469.

21. Council of Europe. History of Artificial Intelligence. Last accessed 23 Sept. 2021. URL: https://www.coe.int/en/web/artificial-intelligence/history-of-ai.

22. World Intellectual Property Organization. Artificial Intelligence and Intellectual Property. Last accessed 23 Sept. 2021. URL: https://www.wipo.int/about-ip/en/frontier_technologies/ai_and_ip.html.

23. World Intellectual Property Organization Secretariat. Third Session: WIPO Conversation on Intellectual Property (IP) and Artificial Intelligence (AI). Geneva. (2020, November 4). Last accessed 23 Sept. 2021. URL: https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_3_ge_20/wipo_ip_ai_3_ge_20_inf_5.pdf.

24. Organisation for Economic Co-operation and Development. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Last accessed 23 Sept. 2021. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

25. The Council of Europe Ad hoc Committee on Artificial Intelligence. Glossary. Last accessed 23 Sept. 2021. URL: https://www.coe.int/en/web/artificial-intelligence/glossary.

26. European Commission. 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. Brussels. 25.4.2018 COM (2018) 237 final, {SWD(2018) 137 final}.

27. European Commission. White Paper on Artificial Intelligence — A European approach to excellence and trust. Brussels. 19.2.2020 COM (2020) 65 final. Last accessed 23 Sept. 2021. URL: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

28. European Commission. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. Brussels. COM(2021) 206 final, 2021/0106(COD). Last accessed 23 Sept. 2021. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

29. European Commission, Directorate-General for Communication. High-Level Expert Group on Artificial Intelligence, a definition of AI: Main capabilities and scientific disciplines. (2018, December 18). B-1049 Brussels. Last accessed 23 Sept. 2021. URL: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf.

30. John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115—232, 132 Stat. 1636, 1695 (2018, August 13) (codified at 10 U.S.C. § 2358, note). Last accessed 23 Sept. 2021. URL: https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf.

31. DAAX. (2020, November 30). The Best Offshore Development Countries in 2021: a 360 Degree Overview. Last accessed 23 Sept. 2021. URL: https://www.daxx.com/blog/development-trends/best-offshore-development-countries-2021.

32. Shearer, E., Stirling, R., Pasquarelli, W. (2020). Government AI Readiness Index 2020. Report by Oxford Insights. Last accessed 23 Sept. 2021. URL: https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/5f7747f29ca3c20ecb598f7c/1601653137399/AI+Readiness+Report.pdf.

33. Council of Europe. Ad hoc Committee on Artificial Intelligence (CAHAI). Last accessed 23 Sept. 2021: https://www.coe.int/en/web/artificial-intelligence/cahai

34. International Organization for Standardization. Standardization in the area of Artificial Intelligence. ISO/IEC JTC 1/SC 42. Last accessed 23 Sept. 2021: https://www.iso.org/committee/6794475.html

35. The Cabinet of Ministers of Ukraine «The Concept for the Development of Artificial Intelligence in Ukraine». (2020, December 02), № 1556-p. Last accessed 23 Sept. 2021. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-p?lang=en#Text.

36. Groberman, R. (2020, April 29). How AI Will Redefine the Way We Think About Ownership. Medium. Last accessed 23 Sept. 2021. URL: https://medium.com/swlh/how-ai-will-redefine-the-way-we-think-about-ownership-e0821c6b2f30.

37. Stephens, K. (2019, December). Who Owns an AI-generated Invention? Twobirds.com. Last accessed 23 Sept. 2021. URL: https://www.twobirds.com/en/news/articles/2019/global/who-owns-an-ai-generated-invention.

38. Thomson Reuters, the Answer company. (2019). Expert Q&A on Artificial Intelligence (AI) Licensing. Last accessed 23 Sept. 2021. URL: https://www.mayerbrown.com/-/media/files/news/2019/01/expert-qanda-on-artificial-intelligence-ai-licensing-w0219801.pdf.

39. Responsible AI Licenses. The Problem. Licenses. Last accessed 23 Sept. 2021. URL: https://www.licenses.ai/about.

40. Responsible AI Source Code License. Template Responsible AI Source Code License Version 1.0, (2019, February 12). Licenses. Last accessed 23 Sept. 2021. URL: https://www.licenses.ai/source-code-license.

41. Responsible AI End-User License. Template Responsible AI end User License Agreement. Licenses. Last accessed 23 Sept. 2021. URL: https://www.licenses.ai/enduser-license.

42. Eisner, R., Peterson, B., Brown, M. (2019, July 04). United States: Smart Licensing of Artificial Intelligence. Mondaq. Last accessed 23 Sept. 2021. URL: https://www.mondaq.com/unitedstates/fin-tech/821656/smart-licensing-of-artificial-intelligence.

43. Lizarralde, M. D. A Guideline to Artificial Intelligence, Machine Learning and Intellectual Property. (2020, September). 4iP Council. Last accessed 23 Sept. 2021. URL: https://www.4ipcouncil.com/application/files/9016/0017/8691/A_Guideline_to_Artificial_Intelligence_Machine_Learning_and_Intellectual_Property.pdf.

44. Fitzgerald, N., Martyn, E., McClenahan, A. Introduction to the protection of IP rights in artificial intelligence. (2019, September 25). Last accessed 23 Sept. 2021. URL: https://www.ashurst.com/en/news-and-insights/insights/ip-focus-on-ai-introduction-to-protection-of-ip-rights-in-artificial-intelligence/.

45. Calvin, N., Leung, J. Working? P?aper: Who owns artificial intelligence? A preliminary analysis of corporate intellectual property strategies and why they matter. (2020, February). Centre for the Governance of AI Future of Humanity Institute, University of Oxford. Last accessed 23 Sept. 2021. URL: https://www.fhi.ox.ac.uk/wp-content/uploads/Patents_-FHI-Working-Paper-Final-.pdf.

46. Guadamuz A. Artificial intelligence and copyright. (2017, September). World Intellectual Property Organization. Last accessed 23 Sept. 2021. URL: https://www.wipo.int/wipo_magazine/en/2017/05/article_0003.html.

47. AIArtists.org. Frequently Asked Questions About AI Art: Can AI create art? (2019). Last accessed 23 Sept. 2021. URL: https://aiartists.org.

48. Planck M. Artificial Intelligence Generated Artwork Sells for $432,500 — Is AI a Simple Tool or Creative Genius? (2021, January 30). Institute for Human Development. Last accessed 23 Sept. 2021. URL: https://scitechdaily.com/artificial-intelligence-generated-artwork-sells-for-432500-is-ai-a-simple-tool-or-creative-genius/.

49. Abbott R. The Artificial Inventor Project (2019, December). World Intellectual Property Organization. Last accessed 23 Sept. 2021. URL: https://www.wipo.int/wipo_magazine/en/2019/06/article_0002.html.

50. Schuster W. M. Artificial Intelligence and Patent Ownership, Volume 75, Issue 4 Washington and Lee Law Review (2019, February 02). 1945-2005. Last accessed 23 Sept. 2021. URL: https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=4627&context=wlulr.

51. Alice Corporation Pty. Ltd. v. CLS Bank International et al. Supremecourt.gov. № 13—298. 1—17. United States Supreme Court. June 19, 2014. Last accessed 23 Sept. 2021. URL: https://www.supremecourt.gov/opinions/13pdf/13-298_7lh8.pdf.

52. PurePredictive, Inc. v. H2O.AI, Inc. Patentnext.com. № 17-cv-03049-WHO. 1-7. United States District Court, N.D. California. August 29, 2017. Last accessed 23 Sept. 2021. URL: https://www.patentnext.com/wp-content/uploads/sites/502/2021/03/Purepredictive-Inc.-v.-H2O.AI-Inc.-2017-WL-3721480-N.D.-Cal.-Aug.-29-2017.pdf.

53. Shubei Zhang, S., An, Z. (2020, September 07). Can AI be an inventor? ManagingIP. Last accessed 23 Sept. 2021. URL: https://www.managingip.com/article/b1n8qgn4h2t8vw/can-ai-be-an-inventor.

54. United States Patent and Trademark Office. (2020, January 20). Decision on Petition. Last accessed 23 Sept. 2021. URL: https://www.uspto.gov/sites/default/files/documents/16524350_22apr2020.pdf?utm_campaign=subscriptioncenter&utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term=.

55. European Patent Office: European Patent Register. Chronological order of all S. Thaler's documents (search/examination, appeal procedures). Last accessed 23 Sept. 2021. URL: https://register.epo.org/application?number=EP18275163&lng=en&tab=doclist.

56. UK Intellectual Property Office. (2019, December 04). Decision BL O/741/19 04. Last accessed 23 Sept. 2021. URL: https://www.ipo.gov.uk/p-challenge-decision-results/o74119.pdf.

57. Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K. & Scharre P. (2018, July). Artificial Intelligence and International Security. Report is part of the Center for a New American Security's series on Artificial Intelligence and International Security. Last accessed 23 Sept. 2021. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/CNAS_AI% 20and% 20International% 20Security.pdf.

58. Comiter M. (2019, August). Attacking Artificial Intelligence: AI's Security Vulnerability and What Policymakers Can Do About It. Paper — Belfer Center for Science and International Affairs, Harvard Kennedy School. Last accessed 23 Sept. 2021. URL: https://www.belfercenter.org/publication/AttackingAI.

59. Congressional Research Service: Artificial Intelligence and National Security (2020, November 10). Last accessed 23 Sept. 2021. URL: https://fas.org/sgp/crs/natsec/R45178.pdf.

60. Weekly Focus, VisionIas: Inspiring Innovation. Artificial Intelligence and National Security. Last accessed 23 Sept. 2021. URL: https://d19k0hz679a7ts.cloudfront.net/value_added_material/Artificial-Intelligence-and-National-Security.pdf.

61. Parsa C. A., the Al Organization, Inc., Victims of Persecution, Rape, Torture, Concentration Camps, Sex, Human and Organ Trafficking and Organ Harvesting in China, Hong Kong, America and Around) and others v. Google L.L.C, Facebook Inc, DeepMind Inc., Alphabet Inc, Neuralink Inc, Tesla Inc, Larry Page, Sergey Brin, Sundar Pichai, Mark Zuckerberg, Elon Musk, CISON PR Newswire & John Doe's 1-29. Digitalcommons.law.scu.edu. № '19CV2407 CAB AHG. 1-49. United States District Court Southern District of California. 2019, December 19. Last accessed 23 Sept. 2021. URL: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3104&context=historical.

62. Ministry of Defence of Ukraine Ministry of Education and Science of Ukraine: Central Research Institute of Arms of the Armed Forces of Ukraine. Coordination Problems of Military Technical and Devensive Industrial Policy in Ukraine. Weapons and Military Equipment Development Perspectives. VII International Scientific and Practical Conference (2019, October). Last accessed 23 Sept. 2021. URL: https://mon.gov.ua/storage/app/media/innovatsii-transfer-tehnologiy/publikatsiyi/2019/10/ta-bezpeka-2019-english.pdf.

63. Osoba O. A., Welser, W. IV. The Risks of Artificial Intelligence to Security and the Future of Work. (2017). RAND Corporation, PE-237-RC. Last accessed 23 Sept. 2021. URL: https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE237/RAND_PE237.pdf.

64. Taniel, G. A., Chan, T. Artificial Intelligence and National Security. (2017). Study: Belfer Center for Science and International Affairs Harvard Kennedy School. Last accessed 23 Sept. 2021. URL: https://www.belfercenter.org/sites/default/files/files/publication/AI% 20NatSec% 20-% 20final.pdf.

65. Buchanan B. The AI Triad and What It Means for National Security Strategy. (2020, August). The Center for Security and Emerging Technology. Last accessed 23 Sept. 2021. URL: https://cset.georgetown.edu/wp-content/uploads/CSET-AI-Triad-Report.pdf.

Жигалова К. С. Отдельные аспекты необходимости правового регулирования искусственного интеллекта в Украине.

В данной статье рассмотрены и приведены конкретные и актуальные аспекты необходимости правового регулирования искусственного интеллекта (ИИ) в Украине. Целью исследования было продемонстрировать конкретные юридические и объективные причины необходимости и целесообразности создания законодательства относительно продвижения, развития и использования искусственного интеллекта (ИИ) в Украине. В разделе 1 «Понимание искусственного интеллекта» приведены примеры применения, доктринальные и различные правовые определения ИИ. Это исследование демонстрирует различные подходы и видения создания наиболее точной терминологии ИИ. В этой главе объясняются ключевые различия между двумя видами ИИ («сильный ИИ» и «слабый ИИ»). Более того, в данном научном исследовании подробно описано и проиллюстрировано различия между такими сложными отраслями техники (технологии), как искусственный интеллект и робототехника. Раздел 2 «Необходимость и целесообразность правового регулирования искусственного интеллекта в Украине» демонстрирует необходимость правового регулирования, иллюстрирует пробелы в действую-

щем законодательстве. Интеллектуальная собственность (ИС) является наиболее уязвимой сферой и требует создания специального законодательства об ИИ. Этот раздел показывает, что чрезвычайно важным является установление защиты прав ИС в рамках правоотношений в сфере ИИ в Украине в следующих аспектах: договорной защите прав интеллектуальной собственности разработчиков ИИ; защита прав интеллектуальной собственности на компоненты ИИ и непосредственно программы ИИ; защиту ИИ и изобретения, созданные ИИ (в порядке охраны и защиты авторских прав); патентная защита (патентоспособность) ИИ и изобретений, созданных ИИ. Также в Разделе 2 анализируются отдельные вопросы ИИ и национальной, международной и социальной безопасности, вопросы защиты данных. Раздел 3 «Вывод» демонстрирует, что отсутствие специального правового регулирования в сфере ИИ (нормативно-правового акта и специального законодательства в сфере ИИ, которое бы регулировало продвижение, развитие и использование искусственного интеллекта в Украине) потенциально может привести к многочисленным проблемам в государственном/частном секторах, может создавать угрозы для экономики, бизнеса, гражданского населения.

Ключевые слова: *искусственный интеллект (ИИ), правовое регулирование ИИ, защита прав интеллектуальной собственности (ИС), национальная безопасность, защита прав и свобод человека, защита данных.*

Жигалова К. С. Окремі аспекти необхідності правового регулювання штучного інтелекту в Україні.
У даній статті розглянуто та наведено конкретні та актуальні аспекти необхідності правового регулювання штучного інтелекту (ШІ) в Україні. Метою дослідження було продемонструвати конкретні юридичні та об'єктивні причини необхідності та доцільності законодавства щодо просування, розвитку та використання ШІ в Україні. У Розділі 1 «Розуміння штучного інтелекту» наведені приклади застосування, доктринальні та різноманітні правові визначення ШІ. Це дослідження демонструє різні підходи та бачення створення найточнішої термінології ШІ. У цій главі пояснюються ключові відмінності між двома видами ШІ («сильний ШІ» та «слабкий ШІ»). Більше того, у даному науковому дослідженні детально описано та проілюстровано відмінності між такими складними галузями техніки (технології) як штучний інтелект та робототехніка. Розділ 2 «Необхідність та доцільність правового регулювання штучного інтелекту в Україні» показує необхідність правового регулювання, ілюструє прогалини в чинному законодавстві. Інтелектуальна власність (ІВ) є найбільш вразливою сферою і прагне до створення спеціального законодавства про ШІ. Цей розділ демонструє, що надзвичайно важливим є встановлення захисту прав ІВ у рамках правовідносин у сфері ШІ в Україні в таких аспектах: договірний захист прав інтелектуальної власності розробників ШІ; захист прав інтелектуальної власності на компоненти ШІ та безпосередньо програми ШІ; захист ШІ та винаходи, створені ШІ (в порядку охорони і захисту авторських прав); патентний захист (патентоспроможність) ШІ та винаходів, створених ШІ. Також у Розділі 2 аналізуються окремі питання ШІ та національної, міжнародної та соціальної безпеки, питання захисту даних. Розділ 3 «Висновок» демонструє, що відсутність спеціального правового регулювання у сфері ШІ (нормативно-правового акта та спеціального законодавства у сфері ШІ, яке б регулювало просування, розвиток та використання ШІ в Україні) потенційно може призвести до численних проблем у державному/приватному секторах, створювати загрози для економіки, бізнесу, цивільного населення.

Ключові слова: *штучний інтелект (ШІ), правове регулювання ШІ, захист прав інтелектуальної власності (ІВ), національна безпека, захист прав і свобод людини, захист даних.*