Observance of Human Rights in the Use of AI as Technology

Submitted: 14 January 2022
Revised: 28 January 2022
Accepted: 29 March 2022

Olha I. Kosilova*
https://orcid.org/0000-0002-5574-3771
Olha V. Rozghon**
https://orcid.org/0000-0001-6739-3927
Chrystyna K. Solodovnikova***
https://orcid.org/0000-0002-9169-9026
Volodymyr M. Stolbovyi****
https://orcid.org/0000-0002-4095-2570
Olha O. Barabash*****
https://orcid.org/0000-0003-2666-9696

Article submitted to peer blind review

DOI: https://doi.org/ 10.26512/lstr.v14i2.41558

Abstract

[Purpose] The purpose of article is devoted to the study of the specifics of legal regulation, use and development of Artificial Intelligence (AI) and related issues of respect for fundamental human rights in modern Ukraine and the EU.

[Methodology] The normative bases of legal regulation of relations in the field of AI are considered. One of the methods, used in this article, is establishment of such general rules for the use of AI that could not violate fundamental human rights.

[Practical Implications] The practical significance lies in establishment that the use of AI is a multi-vector phenomenon that affects all spheres of human life and can violate various groups of rights

[Findings] It was concluded that in order to regulate the use of AI, states need to pay attention to and take into account the Recommendations on AI developed by the European Commission and find a compromise approach to the use of AI, which provides for respect for fundamental human rights.

* Olha I. Kosilova is a PhD in Political Science, Associate Professor at the Research Department, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. Address: 01033, 60 Volodymyrska Str., Kyiv, Ukraine. E-mail: kosilova7287-1@university-of-law.in.net.

** Olha V. Rozghon is a PhD in Law, Leading Researcher at the Department of Legal Support for the Functioning of the National Innovation System, Scientific and Research Institute of Providing Legal Framework for the Innovative Development of the National Academy of Legal Sciences of Ukraine, Kharkiv, Ukraine. E-mail: rozghon@u-tokio.eu.

*** Chrystyna K. Solodovnikova is a PhD in Psychology, Lawyer at the Research Department, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine. E-mail: solodovnikova@lund-univer.eu.

**** Volodymyr M. Stolbovyi is a Full Doctor in Law, Professor at the Department of Civil Law Disciplines, National Academy of Security Service of Ukraine, Kyiv, Ukraine. E-mail: stolbovyi@nanyang-uni.com.

***** Olha O. Barabash is a Full Doctor in Law, Professor at the Department of General Law Disciplines, Lviv State University of Internal Affairs, Lviv, Ukraine. E-mail: barabash@singapore-uni.com.

Keywords: Digital Economy. International Legal Regulation. Protection of Rights and Freedoms. Civil Law. Privacy.

INTRODUCTION

Due to the active introduction of digital technologies and digitalization the "digital economy" is in the process of development, AI technologies are being introduced in security and defense, public administration, the quality and speed of administrative and medical services is improving, the use of digital technologies in various forms of political citizen participation is increasing (from the creation of electronic appeals, petitions, to full-fledged elections and referendums). Simultaneously despite the perception of AI as a successful and popular digital technology, its application in various spheres of public life (economic, social, political, cultural, etc.) must be in compliance with basic human rights enshrined in international documents. This is due to the existence of a certain conflict of interest of entities that want economic growth, automation, and therefore human replacement, and respect for human rights, freedoms and interests, as there is a threat to human rights in connection with the use of AI technologies. Violations of human rights related to the use of AI, namely, dissemination of personal data, interference with the right to privacy, infringement of freedom of expression, are enshrined in the Convention for the Protection of Human Rights and Fundamental Freedoms.

The lack of an appropriate systemic legislative framework for the use of AI requires the search for ways to overcome risks and threats to human rights restoration of violated rights and minimization of threats. Of course, the innovations introduced by the subjects exist in the process of their innovative activities. And digital technologies as a kind of innovative technologies affect the spheres of human life. Therefore, the understanding of the importance of intensive implementation of the latest technologies is reflected in the relevant development strategies focused on sustainable economic growth and strengthening the competitive position of an individual country in the global economic environment. A significant role in innovation is played by digital technologies, which use electronic equipment and allow accelerating and facilitate various processes (PONOMARENKO, 2018).

In the context of law in foreign science, digitalization is seen as a natural phenomenon that arises in the development of the legal system at the present stage (MARK and GURCHETAN, 2014). Digitization – the saturation of the physical world with electronic-digital devices, tools, systems, and the establishment of electronic-communication exchange between them, which actually forms an integrated interaction of virtual and physical – cyberspace. The main purpose of digitalization is to improve through the digital transformation of existing and creation of new sectors of the economy, as well as the transformation of spheres of life into new, more efficient, and modern. Digitization of the real sector of the

economy is a key component of the digital economy leading to the emergence of new products and services, platforms and innovations (ORDER OF THE CABINET…, 2018). Numerous researchers from various scientific fields in the seventh world are engaged in the analysis of the concept of "digital technologies" today.

In this study the authors used the definition proposed by M. Spitzer (2014) in the work "Anti-brain", see more details in it. The digital economy is the basis of the Fourth Industrial Revolution (Industry 4.0.). The term "Fourth Industrial Revolution" was introduced in 2011 as part of Germany's national high-tech strategy and updated in 2020. This strategy concerns the concept of smart manufacturing, which is based on the global industrial Internet of Things and Services. Industry 4.0 involves the introduction of new digital technologies, such as robotics, AI the Internet of Things, augmented reality, and others. AI is a subject of computer science, and the technologies created on its basis are information technologies that allow to perform intelligent reasoning and action with the help of computing systems and other artificial devices (OSIPOV, 2001). The purpose of article is devoted to the study of the specifics of legal regulation, use and development of AI and related issues of respect for fundamental human rights in modern Ukraine and the EU.

DEMAND FOR AI AS DIGITAL TECHNOLOGY

AI as an Integral Part of Industry 4.0

If we consider AI as digital technology, then its difference from conventional software is the speed of calculations of a significant amount of new quality data due to advanced algorithms (ROZGHON, 2020). Many researchers point to the benefits, but also express concerns about the introduction of digital technologies listed in Industry 4.0. Thus, Schwab points out that previous industrial revolutions have freed humanity from animal power, made mass production possible, and provided digital opportunities to billions of people. However, this Fourth Industrial Revolution is fundamentally different (INDUSTRY 4.0…, 2019). It is characterized by a number of new technologies that combine the physical, digital and biological worlds, affecting all disciplines, economies and industries, and even challenge the idea of what it means to be human. AI is already widely used today and partially helps people to a great extent. Siri, Cortana and Alexa voice assistants are based on this concept, as are online navigation systems (Google Maps), online translator (Google Translate, Microsoft Translator) or car parking assistants (VW, Mercedes, Lexus).

As a result, shifts and failures mean that we live in times of great hope and great danger. There is the potential in the world to connect billions of people to digital networks, significantly increase the efficiency of organizations and even manage assets in a way that helps restore the environment, potentially repairing the damage caused by previous industrial revolutions. However, Schwab also has serious concerns: organizations may be unable to adapt; governments may not use

and regulate new technologies for profit; a change of government will create new important security issues; inequality may increase. The Fourth Industrial Revolution is characterized by a much more widespread and mobile Internet, more compact and powerful sensors that have become cheaper, as well as AI and machine learning (INDUSTRY 4.0…, 2019). AI is expected to be a feature of the Fourth Industrial Revolution. AI as a technology and an integral part of Industry 4.0 is interpreted as a term used to describe machines that perform human-like cognitive functions such as learning, understanding, reasoning, or interacting (JAUME-PALASÍ and SPIELKAMP, 2018).

Extreme auto communication with AI can increasingly automate some skills that only humans previously had. AI will be the most successful in processing big data, potentially including speech and image processing, which have so far been banned for computers. Extraordinary automation can allow the introduction of more robots and AI for production, analysis of results, complex decision-making and adapt conclusions to environmental factors (EXTREME AUTOMATION…, 2016). With the development of digital technology and automation, Alibaba Group CEO Jack Ma is also thinking about future economic growth. According to him, governments and businesses need to stop relying on production in terms of job creation, and pay attention to innovative industries – such as developments in the field of AI. We all greatly underestimate the biggest technological revolution that is happening right now. The world is moving from IT to DT. Many do not understand what DT is (just as many do not know what IT is). Information technology (IT) is gradually shifting to data technology (DT).

O. Karpenko (2017) says: "We are no longer talking about another technological upgrade, we are talking about philosophy, about our approach to tasks. Many people, when talking about increasing the number of jobs, mean production. Production will never create many jobs. This has worked in the past. But in today's world, due to new technologies such as AI, robots, production will never regain this role. The main driver of job creation will be the service industry". In most developed countries, information and communication technologies have been identified as the main means of modernizing government activities to increase efficiency, provide public services, including access to information on the activities of state and municipal authorities. Administrative mechanisms of e-democracy and e-government have been included in the reforms of government models, which has also significantly affected the form of international communications. National services for citizens of some countries have become available to citizens of others. Such a model of international relations is much more transparent and more attractive for political, economic, cultural and social connections with countries with developed national information segments (HRYTSIAK and SOLOVYOV, 2013).

Different countries have different priorities in the field of digital transformation, for example, China in its program "Internet Plus" integrates digital industries with traditional, Singapore forms a "Smart economy", Canada creates an ICT hub in Toronto, which is driven by ICT, and South Korea in the "Creative Economy" program focuses on human capital development,

entrepreneurship and the dissemination of ICT achievements, Denmark focuses on the digitalization of the public sector. Digitalization has manifested itself most vividly in Singapore. There, in 2014, the state initiated the development of the concept of a "smart nation" and invited the business and expert community to cooperate for its improvement and implementation. In May 2017, Singapore's AI program was launched for 5 years. It is a nationwide partnership involving six different organizations. The goals of the program are to invest in the next wave of AI research, to address key social and economic issues, and to introduce and use AI in industry (KRAKOVETSKY, 2018). According to V. Zagariy et al. (2019): "Digitalization, AI and robotics will be the main drivers of global economic growth in 2030 and this will be due to full automation of processes, increased productivity and the introduction of fundamentally new business models and technologies as digital platforms, digital ecosystems, "Industry 4.0 technologies".

Breakthrough technologies, including AI, are expected to be able to solve many of the social problems associated with meeting basic human needs. The purchasing power of the population will increase. New segments related to creative realization and leisure of people will be created, new types of demand for unusual goods and services will appear. Over the past two years, Canada, Japan, Singapore, China, the UAE, Finland, Denmark, France, the United Kingdom, the European Union Commission, South Korea and India have implemented strategies to promote the development of AI. Digitalization and new technologies will also affect the conditions of competition in the world. By involving AI and robots in production processes and services, the cost of labor will become a less important factor in determining the country's competitiveness, and technological competence and quality of infrastructure, on the contrary, more important. The size of the economy and the well-being of the citizens of each country in 2030 will depend on how much money will be invested in innovation over the next 10 years, with what intensity it will happen (FORECAST OF THE WORLD…, 2018). Since Industry 4.0 involves the widespread introduction of AI into the economy, let's take a closer look at this digital technology.

Trends in the Development of AI: Problematic Issues and Prospects

It is necessary to specify the definitions of AI proposed in international documents. According to the definition given in the European Parliament resolution, "AI" is a "smart robot", which has the following features: acquires autonomy through sensor sensors and/or through data exchange; independently studies experience or interaction; has little physical support; adapts the model of behavior to the environment; is inanimate in the biological sense (EUROPEAN PARLIAMENT RESOLUTION…, 2017). According to the European Commission (COMMUNICATION FROM…, 2018), AI is interpreted in terms of systems that demonstrate mental activity in the form of environmental analysis and taking measures – with some degree of autonomy – to achieve a specific goal. AI-based systems are either purely software used in the virtual world (voice assistants, image analysis software, search engines, speech and face recognition

systems, etc.), and AI can be embedded in hardware devices (advanced, stand-alone machines, drones or the Internet of Things).

When defining AI, researchers are based on the concept of rationality, because to select the most appropriate actions needed to achieve a certain goal, certain criteria are taken into account, which need to be optimized, while having available resources (A DEFINITION OF AI…, 2019). The North Atlantic Treaty Organization (NATO) pays considerable attention to AI technologies and the practical aspects of their application and use in terms of compliance with national priorities, as well as fully takes into account the possible problems associated with the widespread use of relevant technologies in the world. AI technologies are information technologies using AI. Fundamental AI technologies are designed to promote the transformation of the economy, labor market, government agencies and, consequently, society as a whole. The use of AI provides significant opportunities in various spheres of social and economic life, namely – increasing production efficiency, reducing costs, improving the quality of goods and services. The growth of the data array, the creation of new types of sensors and the reduction of computing power creates the preconditions for the further development of AI (ORDER OF THE CABINET…, 2020).

AI contains 5 types of technologies: computer vision, speech reproduction, virtual assistants, automated (robotic) work and the latest machine learning. It is noted that by 2030, 70% of companies will implement at least one of these technologies. In particular, the level of development of artificial intelligence and robotics technologies allows introducing assistant robots into everyday life. For example, the level of development of AI and robotics technologies allows the introduction of assistant robots into everyday life. Even now, in industrial shops, workers often have to work alongside collaborative robots, loader robots are used in warehouses, and vacuum cleaners – in the household. The production of autonomous vehicles that require people management has begun (FILIPOVA, 2020). As we can see, this is a kind of virtual assistant that replaces a person.

This provides more capacity, time and budget, and increases the accuracy of the information needed to manage people. AI helps to effectively automate most of the functions of the back office and services with the help of technological chatbots (BAY, 2019). The authors assume that AI is gradually replacing the worker in the field of labor, performing certain labor functions previously performed by the worker. Robots that are endowed with AI already today perform certain types of work and provide a ready-made product or service. Examples are information retrieval, its processing and systematization, navigation, and so on. Thus, the development of digital technologies affects the labor market and changes the labor process. A new object appears – AI, which in the regulation of its status and in certain areas of life of economic entities can become a subject (AZMUK, 2019). As a preliminary conclusion, the authors note that since AI can predict human behavior, it can lead to the replacement of the human worker, and, consequently, lead to a certain percentage of unemployment. J. Miller (2018) pointed out the problem and risks of uncontrolled development

and use of AI: "AI is now being transformed into a kind of mind, that is, endowed with purely human traits".

Developers of Google's input/output devices have unveiled their new Duplex system, which is an AI-based virtual assistant that can make phone calls to optimally organize the schedule of its "boss". And there was also the question of empathy and whether the machine can sympathize with someone? Machines cannot mentally identify with humans because what happens in our human mind includes things that a machine will never be able to experience on its own, no matter how advanced and profound its own analytical processes and sensory perceptions may be (RENTYUK, 2019a). E. de Haro (2018) is thinking: "It is much more complicated when machines begin to make decisions that have serious consequences, without the emotional context and common values that people use in such cases. For example, an unmanned vehicle, which must decide in the event of an imminent accident – to kill a parent or child. Will such a machine ever be able to explain to people why it makes this or that choice? And if it is not necessary to prove the actions of the machine by human consequences and from a human point of view, what will happen to our system of ethics and justice?"

In fact, AI can mimic human actions, but in the narrow sense, with an understanding of the robot. And this is based on the "concept of limited or narrow AI". And means a program or system capable of performing a set of specific tasks without human intervention. Such AI is significantly different from general AI, which is commonly seen in movies and TV series, and which has independent human capabilities (RENTYUK, 2019b). Due to economic growth in developed countries, there is a growing interest in research in the field of AI, while paying attention to human security. The European Union (EU) is taking many steps to ensure the responsible use of technologies. The EC (2020) has set up the European Group on Ethics in Science and New Technologies (EGE) (2016) to reflect and advise the Commission on ethics, fundamental and social rights arising from the evolution of science and technology: AI, gene editing or the future of robots. The EC promotes a European approach to AI and robotics, which is based on three principles: connecting and strengthening AI research centers in Europe; support for the implementation of an "on-demand AI platform", that will provide access to relevant AI resources in the EU for all users; providing support for research into AI programs in important sectors (EUROPEAN STRATEGY…, 2020). It is advisable to highlight the main advantages and disadvantages of AI. Thus, the advantages of AI include:

– Ability to instantly memorize information and process a huge amount of it in the shortest possible time. In order for any knowledge to settle in a person's mind and not be forgotten, it is necessary to repeat the information for 3-4 days, and then at least once every 1.5 months to refresh it in memory, at least indirectly. AI will remember once and for all.

– Incredibly fast quantitative data processing. By the time a person adds two two-digit numbers, the computer will analyze the economic situation and give a point on the chart where it is best to buy currency. And then it will conclude this transaction itself and exit the market in time, leaving its owner with the profit. A trader cannot handle such an enormous amount of quantitative information.

However, AI has disadvantages: AI is not yet able to process qualitative information, but it's only a matter of time; AI can still fail. It is not so perfect yet, so you still need a person who will "supervise" it. But in a few decades, AI can learn to see its failures, fix them, and a person will not be needed (AI: WHAT IS IT…, 2018).

Human Security vs AI: Ways to Overcome the Conflict

Modern technological solutions related to AI must protect people from the challenges/risks and threats that may be caused by their use or by natural, technological and anthropogenic crises in the world. Therefore, human safety is definitely related to the use of AI. The terms human security was introduced by the United Nations Development Program (UNDP) in 1994 (BRUCE et al., 1994), which stated that "human security is protection against persistent threats such as famine, disease and repression, and includes protection against sudden and dangerous daily risks, at home, at work or in society". The existing National Security Strategy of Ukraine (NSS), which was adopted in 2015, is certainly outdated. There have been attempts to create new versions of the Strategies in Ukraine, but everything remained at the stage of discussing the Projects. The key aspects of this Strategy are the person, his life, health, honor, dignity, inviolability and security. Other strategic planning documents will be prepared and implemented on the basis of the NSS. It is, first of all, about the Strategy of human development, information security, cybersecurity, etc.

Due to the rapid development of AI technologies, information security and cybersecurity are under the greatest risks and threats. Information security is focused on ensuring the security of all information data and covers both data on physical media and information extracted from the data. Cybersecurity focuses on protecting the data used to store and transmit this information in cyberspace, in particular data protection. In view of the above, as well as the growth of public activity in this area, the Global Regulation on Data Protection (GDPR) was adopted. 4 years of preparation and debate and the GDPR was finally approved by the EU Parliament on April 14, 2016, and entered into force on May 25, 2018. Organizations that do not meet these requirements may face large fines. This is the first legal document to have extraterritorial force. All companies that process personal data of entities living in the EU are obliged to comply with these rules, regardless of the location of the company. Prior to the entry into force of this provision, the territorial affiliation of the Directive had ambiguous interpretations and related to data processing "in the context of the territory of the institution".

Not surprisingly, such ambiguity has provoked a number of lawsuits that have found that the General Data Protection Regulation (GDPR) must apply to the processing of personal data by EU performers, whether processed in the EU or abroad. The GDPR also applies to the processing of personal data of EU entities by a controller or processor not established in the EU, where the activity involves offering goods or services to EU citizens (for a fee or free of charge) and monitoring the behavior of these companies in the EU. Non-EU companies that

process EU citizens' data must also appoint a representative in the EU (REGULATION (EU) 2016/679 …, 2016). In 2018, there was an increase in public awareness of the importance of data confidentiality. Mankind has learned that data misuse can cause serious problems due to the scandal with Cambridge Analytica and countless security breaches that reveal user data (FACEBOOK TO BE FINED …, 2019). For example, in San Francisco, authorities have banned the use of face recognition technology in public places, even the police. However, the ban does not mean that this state of affairs is justified (SOROKA, 2019).

California has introduced a similar legal entity – the Consumer Protection Act of 2018, which entered into force in 2020. This law regulates the relationship between companies and their customers in the field of collection and sale of personal data, and companies can give individuals significant rights to their data. In addition, on May 16, 2018, a declaration was signed in Toronto, which provides for the protection of the right to equality and non-discrimination in machine learning systems, and on December 5, 2018 – the Montreal Declaration for the Responsible Development of AI Launched (2018). The Montreal Declaration was developed and implemented as a result of long-term cooperation of experts, lawyers, government officials together with stakeholders, civil society organizations and citizens. The Declaration identifies fundamental ethical values and principles that guarantee the observance and protection of fundamental human rights as the basis for AI and its annexes. It should also be noted that the Committee of Experts on Human Rights in Automated Data Processing and Different Types of AI (MSI-AUT COMMITTEE…, 2020). Committee of experts has released draft documents on the implications of AI proliferation for human rights. The results of these studies and recommendations focus on the implementation of standards and encourage Council of Europe member states to address legislative issues in this area, to take the necessary measures to ensure respect for human rights in the development and implementation of AI.

The Advisory Committee of the Convention for the Protection of Individuals with regard to Personal Data Processing (2018) has published Guidelines on AI and Data Protection (2019). The guidelines are designed to help politicians, developers, manufacturers and service providers of AI. They are designed to oversee AI data protection programs. The CC emphasizes that the protection of human rights, in particular the right to protection of personal data, should be the basis for the development and implementation of AI programs, in particular when they are used in decision-making processes and based on the revised October 2018 Data Protection Convention. Note that any AI innovation should be based on priorities to prevent and reduce potential risks in the processing of personal data, and should allow the subjects of this data to control their processing and its consequences. These AI principles address the important issues outlined earlier in the Guidelines for the Protection of Individuals with regard to the Processing of Personal Data in the World of Big Data and the need to "protect personal autonomy based on the human right to control and process such personal data considered" in this context (NEW GUIDELINES…, 2019).

The use of AI technologies should be based on the rules of cybersecurity and information security laws. The fight against cybercrime is being carried out

in the same direction, where the automation of certain criminal acts is already causing significant damage. The Convention on Cybercrime (2001) of the Council of Europe, also known as the Budapest Convention, has provided a unique basis for judicial cooperation since 2001. This convention has already been ratified by more than 60 countries. Thus, we can talk about the need to protect human rights, data and confidentiality, and the necessary security of the individual by the state as a tool for implementing the Human Development Strategy.

Normative Bases of Legal Regulation of Relations in the Field of AI: International and Domestic Aspect

The problem of normative regulation of issues of development of new digital technologies, including "AI", is topical and debatable, in particular: the legal nature of "AI", possible legal status of AI system of subject of civil law or legal regime as object of civil law is actual and debatable decision-making by "AI" and legal liability for damage caused by AI, as well as intellectual property rights to works as objects of intellectual property created with the participation of AI (ROZGHON, 2020). Obviously, the use of modern advanced AI technologies should not contradict human rights, civil liberties, the principles of the rule of law. T. Fuley (2015) emphasizes: "It is important to realize that the rule of law covers not only the substantive aspect (legal relationship between man and the state on the basis of recognition of human superior social value), but also the procedural aspect, which is based on compliance with law-making and law-enforcement practices, such as: prohibition of retroactive effect of the law, requirement of clarity and consistency of the law; requirement for uniform application of the law; application of punishment solely on the basis of law, etc.". The well-known report of the Venice Commission in 2011(REPORT ON THE RULE…, 2011), in which, based on the analysis of the legal systems of European states, an attempt was made to identify universal for different countries elements of the rule of law. The report proposes at least 6 necessary elements, which must be observed not only formally, but also in essence. These are: legality, including a transparent, accountable and democratic law-making process; legal certainty; prohibition of arbitrariness in decision-making; access to justice by an independent and impartial tribunal, including the possibility to challenge in court; respect for human rights; non-discrimination and equality before the law (FULEY, 2015).

Analyzing the vectors of development of national legislation, it is worth paying attention to the Recommendations of the Organization for Economic Co-operation and Development on AI and adopted by it in June 2019 by the G20 Human-Centered Principles (G20 MINISTERIAL…, 2019), as well as the Coordinated Plan and Ethical Guidelines for Trustworthy AI (ETHICS GUIDELINES…, 2019) developed by the European Commission. The OECD recommendations have two structural components: the principles of good governance of trustworthy AI; national policies and international cooperation. In particular, the document establishes five interrelated principles: growth, sustainable development and prosperity; humancentered values and justice;

transparency and clarity; reliability, protection and security; responsibility. The Coordinated Plan of the European Commission (COORDINATED PLAN…, 2018), in addition to strengthening technological and industrial capacity, provides a legal and ethical framework that is in line with the values of the European Union and the EU Charter of Fundamental Rights. These documents reflect current trends in the processing of personal data, with an emphasis on ethics and human rights protection. At the same time, the highest priorities are freedom, dignity, autonomy, privacy, nondiscrimination, equality, social justice and labor rights. The Council of Europe's conclusions on the Game Policy Management Conference – the impact of AI on human rights, democracy and the rule of law – emphasize the need to inform citizens about the opportunities and potential risks of AI, fostering public confidence in the information environment and AI (ALEKSIUK, 2019).

Moreover, the conclusions speak of algorithmic transparency, equality before the law, which cannot be violated by the algorithm, as well as the inviolability of existing important international documents – the Universal Declaration of Human Rights and the Convention for the Protection of Human Rights and Fundamental Freedoms (ALEKSIUK, 2019). On February 19, 2020 The EC has published a White Paper (2020), on strengthening the European ecosystem of best practices and trust in AI and a Report on aspects of AI safety and responsibility to ensure an appropriate ethical and legal framework (REPORT ON THE SAFETY…, 2020). The White Paper discusses measures to optimize research, cooperation between Member States and increase investment in AI; government tools of the EU regulatory framework, which will determine the types of legal requirements that will apply to the relevant entities, with special emphasis on high-risk applications. Therefore, trust in human-oriented AI technologies needs to be strengthened and an international consensus on AI (WHITE PAPER…, 2020). Given that AI systems can be beneficial to humanity, but at the same time cause fundamental ethical issues that can lead to inequality, isolation and threats to cultural and social diversity and gender equality and their potential impact on privacy, freedom of speech, social, economic and political processes and the environment, etc. Ad Hoc Expert Group (AHEG) has prepared a draft text of the recommendation on ethical aspects of AI as an international normative act on ethical aspects of AI in the form of a recommendation (UNESCO LAUNCHES…, 2019).

The recommendations set out the values and principles of AI application identify areas for policy action and monitor and evaluate the ethical component of UNESCO's AI policy it is cautioned that AI cannot be granted legal personality therefore the responsibility for the decisions taken by the AI rests with the individual or legal entity and this should be reflected in the legal framework of United Nations Educational, Scientific and Cultural Organization (UNESCO) member states. The UNESCO expert group is reviewing the draft text of the Recommendation on the ethics of AI. The lack of an integrated approach to the interaction of AI and humans undermines our very existence, the way we learn, think and even make decisions. Exclusivity and cultural hegemony in the design of AI systems and their potential benefits put vulnerable people even more at risk.

UNESCO wants to create an instrument that includes the voices of the Global South, youth, women and other underrepresented groups, and will promote fundamental values that leave no one behind. The principles and policies identified in the process will be universal and intergenerational, providing a basis for a common framework to ensure the rule of law on the Internet and in the wider digital world (UNESCO'S EXPERT…, 2020).

According to experts, the COVID-19 outbreak further exposed AI vulnerabilities, digital divide and inequality of opportunity. Developing countries are likely to be more modest due to much lower rates of implementation of AI technologies, lack of ownership of such technologies and often not active participation in design and development processes, but rather recipients of technologies. Economic growth is likely to be strongest in China and North America, accounting for nearly 70 percent of AI's global economic impact (UNESCO'S EXPERT…, 2020). As a result of the work of the expert group, a second draft will be prepared and submitted to UNESCO member states for written comments in September. The Recommendation will then be reviewed during the intergovernmental process and submitted for adoption at the 41st General Conference of UNESCO in November 2021. Therefore, the UNESCO Recommendation is extremely important. It is a starting point for addressing issues such as cultural representation, given the limited resources of low – and middle income countries, confidentiality and data protection, increased surveillance, racial bias and increased misinformation. The ultimate goal is to ensure that AI is designed and used in accordance with the principles of inclusiveness, diversity and transparency.

The European Code of Ethics for the use of AI in the judiciary adopted by the EC of the Council of Europe on the effectiveness of justice in 2018 is an important international legal instrument in the field of legal regulation of AI its main objective is to improve the efficiency and quality of the administration of justice by developing algorithms for judicial decisions and data while respecting the fundamental rights and freedoms guaranteed in particular by the ECTHR and the convention for the protection of individuals with regard to automatic processing of personal data (SHEMSHUCHENKO, 2020). The ethical Charter sets out five principles for the use of AI in the administration of justice: the principle of observance of basic human rights when using AI; the principle of non-discrimination, namely the prevention of the development of any discrimination between individuals or groups of persons; the principle of quality and safety, which relates to the processing of court decisions and data in a secure technological environment; the principle of "under user control"; the principle of transparency, impartiality and fairness (EUROPEAN COMMISSION…, 2018). The Ministry of Digital Transformation of Ukraine has developed and submitted for public discussion the Concept of AI Development in Ukraine (ORDER OF THE CABINET…, 2018). The draft Concept identifies eight key areas of public policy in the field of AI: education and human capital; science and innovation; economics and business; cybersecurity; defense; governance; legal regulation and ethics; justice.

The Concept defines the following main strategic directions of development: development of human capital and emphasis on education of developers in the field of AI (their salaries on the market are twice higher than of ordinary programmers); business development using AI; active introduction of AI technologies in the public sector and major industries of the country; the need to respect the right to privacy (it is planned to develop a Code of Ethics for the use of AI, taking into account European experience). Among the basic principles of development and use of AI technologies in the Concept the following are defined: AI should benefit people and the planet by promoting inclusive growth, sustainable development and prosperity; AI systems are developed and used only under the rule of law, and their use must be ensured by appropriate guarantees, in particular, the possibility of unimpeded human intervention in the functioning of the system; ensuring transparency and responsible disclosure of information about AI systems; organizations and individuals who develop, implement or use AI systems are responsible for their proper functioning in accordance with the above principles (DVOROVY, 2020).

THE IMPACT OF AI ON THE REALIZATION AND IMPLEMENTATION OF HUMAN RIGHTS AND FREEDOMS

Threats to Human Rights Related to the Use of AI Technology

The development of AI technology has already led to the emergence of social problems in the field of labor law, as there is a "substitution effect" and a change in human status in society. The necessary effective human security guarantees that will promote economic development will take into account potential risks, and the use of technology will be subject to normal functioning and management. The use of AI technology and the development of "smart robotics" contributes to the impact on public relations and poses a threat of human rights violations. This affects the private law sector, necessitates a balanced legal settlement of the legal regime/status of robots endowed with AI, prosecution for damage caused by the actions of the robot, as it may violate the rights of other people, and protection and defense of intellectual property rights created by such robots. The widespread use of AI technologies in the world, especially in countries with low levels of socio-economic development, must take into account and protect fundamental human values and rights. The peculiarity of universal rights is their inalienable nature and the possibility of restricting them only by a special procedure.

The Constitution of Ukraine enshrines the principle of universality of human and civil rights and freedoms, which is that the state is accountable to man for his activities, as well as the establishment and protection of human rights and freedoms is the main duty of the state. In addition, man, his life and health, honor and dignity, inviolability and security are recognized in Ukraine as the highest social value; rights and freedoms and their guarantees determine the direction of the state. An important element of Art. 21 of the Constitution of Ukraine is linked

to human dignity, because "all people are free and equal in their dignity and rights" (LAW OF UKRAINE No. 254K/96…, 1996). In general, dignity can be defined as an objective property of a person that reflects his unique, unsurpassed value. In the scientific and practical commentary to the Constitution of Ukraine it is emphasized that human dignity should be interpreted as a right guaranteed by Art. 28 of the Constitution of Ukraine, and as a constitutional value that fills the meaning of human existence, which is the foundation for all other constitutional rights, a measure of determining their essence and a criterion for the admissibility of possible restrictions on such rights (PETRYSHYN et al., 2003).

The right to human dignity is interpreted by modern domestic and foreign researchers as a defining natural human right. In cases of human violation right or freedom, his dignity is always degraded. In Ukraine, there is a right to human dignity seen as equivalent and commensurate with other rights, such as the right to life, freedom, etc. Whereas in other countries, in particular in Germany, the right to human dignity exists the highest constitutional value and the source of all other human rights. In authors` opinion, human dignity should be understood as the idea that all people have the same value regardless of any characteristics (figure), such as origin, gender or age. From a legal point of view from the point of view, the right to human dignity belongs to natural human rights and is one of the main ones' legal values, which serves as a criterion for assessing the constitutionality and legality of the action, action inaction of state bodies and officials, individuals and legal entities. So, the use of AI technology should primarily protect the human right to dignity as the main and a fundamental human right that is the basis for all other rights and freedoms. Violation of any human rights can thus be considered a violation of the right to human dignity.

Analyzing the current directions of development and dissemination of AI technologies, the authors can say that AI will in one way or another affect, or already affects the realization of most human and civil rights and freedoms in the future. The impact of AI is diverse. On the one hand, AI can block content that incites hatred and violence against humanity, but it is also used to suppress the legitimate right to express one's opinion. The use of AI also affects the right to privacy as a result of nontransparent data collection, provision to third parties, disclosure of personal information and tracking of individual users. On the other hand, it is AI that can help detect such abuses (UNESCO LAUNCHES…, 2019). The main prospects for the development of AI as a science and technology:

– advances in AI and automation can lead to the loss of people's jobs – they will be taken away by machines);

– AI will become smarter than hackers because in "other people's hands" their super-intelligent systems will sow chaos and destruction;

– AIs begin to understand people's behavior and make recommendations about what might suit their individual preferences;

– AI becomes like a person and feel his feelings: AI copes with people's actions;

– AI can receive, remember and store large amounts of information, etc.;

– the use of AI in combat operations (for military purposes) will save hundreds of thousands of lives, but a weapon that has a mind and acts independently, poses a threat even to its creators;

– teaching AI human values is a serious danger, because, remembering history, you can find facts that, even by studying examples of "right" and "wrong" behavior, actions of people, etc. (SUKHOTERIN et al., 2018).

Thus, from the whole catalog of rights and freedoms we can distinguish those that are most at risk of violation or already have significant violations due to the use of AI technology. First of all, these are the rights enshrined in the European Convention human rights (ECHR) as the right to a fair trial (Article 6), the right to respect for private and family life (Article 8), freedom of expression (Article 10), the prohibition of discrimination (Article 14), as well as the rights enshrined in the International Covenant on Civil and Political Rights (1966), in particular the right to freedom of movement (Article 12), the right to free and fair elections (Article 25); the right to work (Article 6), enshrined in International Covenant on Economic, Social and Cultural Rights (INTERNATIONAL COVENANT…, 1966). Let's analyze some of the existing threats due to the use of AI in connection with their human rights violations. Monopolization of large social media and accumulation with subsequent use of a significant array of personal data. As a result of this threat, human rights violations such as the loss of privacy of private data on the Internet and interference with personal and private life arise.

The human rights organization Amnesty International has presented a report analyzing the impact of digital life from a human rights perspective. The report focuses on AI algorithms. According to Rasha Abdul-Rahim of Amnesty International, a London-based non-governmental organization, large surveillance corporations such as Google or Facebook are violating the rights to protection of confidential data of a person; they dominate digital life, their services are free, but we pay with our data because: the smarter the system has to work, the more data it needs (KÜNSTLICHE INTELLIGENZ…, 2020). Amnesty International sees the situation as a problem: 90 percent of Internet searches are made through Google, and more than two-thirds of social media users have a Facebook account. Thus, Amnesty International requires investment in alternative Internet models and stricter rules (KÜNSTLICHE INTELLIGENZ…, 2020). This opinion is confirmed by the following statistics: in the modern world there are already 2.3 billion users on Facebook, 2 billion – on YouTube, 1.6 billion – on WhatsApp. Almost half of the planet is part of a virtual community that lives by rules different from the rules of the real world (PAVLYUK, 2019; PYRMA, 2019).

The scandal, which focused on Facebook after the New York Times reported on March 2018 that the British company Cambridge Analytica managed to collect the personal data of tens of millions of Facebook users to develop an algorithm for analyzing voters' political preferences, became widely known around the world. As former employees of the organization told the publication, the created algorithm facilitated the distribution of political advertising to users in order to influence their choice (FACEBOOK IS LATE…, 2020). Michael Lysander Fremuth, research director at the Ludwig Boltzmann Institute for

Human Rights in Vienna, sees the right to information as potentially compromised by AI technology: "Especially when the algorithms display only the target information depending on the user profile and thus act unnoticed as a filter in advance. The right to freedom of expression is also affected when automated programs decide which content can be published or which service providers should remove, for example, for reasons of personal protection" (KÜNSTLICHE INTELLIGENZ…, 2020).

Francois Gave, France's Deputy Permanent Representative to the European Union, emphasized the importance of including the use of AI in the G7 agenda. He noted, in particular, that democracy itself could be threatened because some people do not realize that their information is being collected and stored. At the level of the European Union, there are many principles concerning human rights and data confidentiality. However, he believes that "now is the time to move on and work together" (UNESCO UNVEILS…, 2019). In addition, the draft text of the recommendation on ethics of the Ad Hoc Expert Group on Artificial Intelligence (AHEG) (OUTCOME DOCUMENT…, 2020) previously set increased requirements for the protection of personal data and the preservation of citizens' right to forget. States should pay particular attention to the protection of personal data the disclosure of which could cause harm or moral suffering to a person. These include data on criminal proceedings, crimes, convictions, as well as biometric data, data on race and ethnicity, beliefs, religion, etc.

Control and Restriction of Search Information

Among the techniques used by AI developers when a person uses various Internet resources and social networks it can be identified, in particular, the creation of so-called "information bubbles", or information filters. The mechanism for creating and operating an "information bubble" is as follows: web pages can use algorithms that track what you are looking for, what you click on, what you like or dislike, what you comment on, and where you are. These algorithms analyze all this personal information and use templates to decide exactly what you want to see. This means that search results, links, advertisements and posts on Facebook may be the result of your previous online behavior. In his book, The Filtering Bubble: What the Internet Hides from You, E. Paraiser (2011) emphasizes the risk of being caught in a so-called "soap bubble" because Internet search queries operate on certain filters and algorithms. A paradox arises: the new opportunities provided by the Internet for the development of democracy are more and more limiting us in our own bubbles. We are offered parallel but separate universes. Computer networks are changing the way information flows on the Internet, and it is invisible. And if we don't pay enough attention, it can become a real problem.

There are 57 signals that Google reads – everything from which computer you use, which browser you use to where you are. It uses all this to personalize your search results. You can't see how different your search results are from someone else's results (PARISER, 2011) the 2016 US presidential election, an

investigation by The New York Times found that Facebook users' news feeds are shaped by their political preferences. Such "information bubbles" could well influence people's decisions to support a particular candidate (PAVLYUK, 2019). By doing so, social media and search engines can isolate information that contradicts a person's beliefs. The effect of the information (filtering) bubble limits a person from a variety of ideas and views on events, trends and problems that exist in the world, if it contradicts his preferences. This effect can be avoided by using other search algorithms, so in this case we cannot talk about the violation of the right to information of a person.

Another way to control information is to create fake news or distort information. The developers of Open AI have created AI that can write realistic stories, poems and articles, and based on it created a neural network capable of producing fake news and spam for social networks, according to the BBC. The first version of AI was considered "very dangerous" for open access, so the developers created an algorithm that uses fewer phrases, called GPT-2. It was trained on a database of eight million sites. AI is able to adapt to the style and content of the text that is given to it. AI experts note that the algorithm "works almost well enough to be used to generate texts". However, they are afraid of how this neural network can be used. Tristan Green, author of The Next Web, said about the algorithm the following: "I'm scared of GPT-2 because it's the kind of technology that evil people will use to manipulate the population – and I think it's more dangerous than any pistol" (VAULINA, 2019).

Manipulation of consciousness through the presentation of distorted information is widely used in the election campaign. The use of so-called "bots" and "trolls" controls the information provided to voters, substituting information, and imposing certain ideas and principles that may not be true. Preelection campaigns are becoming increasingly popular on the Internet due to the ability to quickly reach a huge number of potential voters and the cheapness of political advertising. Bots are essentially stand-alone social media accounts, and are programmed to aggressively distribute one-sided political messages to create the illusion of support. The tactic of mass "attacks" of political bots has been repeatedly used in many Western countries, despite the stated principles of "open democracy". The largest cases of bots were used in the 2017 state elections in the United Kingdom, when false information about candidates in favor of the illusory advantages of the least popular candidates for a seat in the government was actively spread on social networks. The same thing happened during the US presidential election in 2016 and during a number of other key political elections around the world (GURIEVA, 2019; CHUBATYUK, 2018).

The use of AI in many areas leads to "new discrimination". Communication takes place between a person and an algorithm without the participation of other people, and it is the algorithm that can now make certain decisions: from a chatbot that will offer the best options for travel, to a robot that will decide whether to let you cross the border or use weapons against you, or hire you (GURIEVA, 2019). As a result, Article 14 of the ECHR on the prohibition of discrimination is violated. Not only the amount of data used for AI systems is sensitive, but also the type of data. "Selfstudy programs are often taught using old

databases. This is problematic because the awareness of discrimination, such as racism and sexism, has never been so pronounced", explains M. Kettemann (KÜNSTLICHE INTELLIGENZ…, 2020), a researcher at the Alexander von Humboldt Institute for Internet and Society in Berlin. One example is the AMS (Alon, Matias, Szegedy) algorithm, which classifies people with or without higher education responsibilities into the worst categories, which specifically affects access to support measures for these people. Due to the widespread use of AI technologies, which seem to be absolutely infallible, automated solutions lose the competence to take into account individual cases of specific people, may not take into account their characteristics and personal qualities and abilities that the machine cannot detect in superficial analysis of factual data.

Another notorious example of programmed bias is the Compas program, which is used in some states to calculate the risk of recidivism among criminals. For Compass, it is important what area a person comes from, what income they have and whether their parents are divorced. The main problem is that when we look at AI technology or other advanced technologies, we tend to think that they will solve all our problems. That they do not possess the prejudice inherent in human judgment. But it's not really that simple (GURIEVA, 2019). AI technologies are based on available data containing racial and gender stereotypes in society, creating the so-called white man problem: AI distinguishes the faces of white people much better, identifying the faces of African Americans and Asians worse (mistakenly defining them as images of animals or squinting people). All because AI is trained mainly by white scientists on the basis of thousands of photos, primarily of white people. This leads to discrimination in areas such as police practices, court decisions or employment (VARAKINA, 2019).

A prerequisite for the introduction of AI in Ukraine is the launch of a single judicial information and telecommunications system (SJITS). In general, the system provides completely paperless record keeping by using electronic digital signatures and electronic document management, creating personal offices to perform any procedural actions, improving the unified state register of court decisions, adding a system of hyperlinks to legal positions of the Supreme Court, which will allow the algorithm to select a relevant decision of the Supreme Court and construct a draft decision without human intervention. It is quite possible that in the future minor disputes can be resolved through the AI system online, which will significantly relieve the courts.

Today, the "Electronic Court" (2020) subsystem operates in a test mode, which provides the exchange of procedural documents (sending and receiving documents) in electronic form between courts, bodies and institutions of the justice system, between the court and litigants, between litigants. With the help of the E-court service, litigants can submit procedural documents (claims, petitions, etc.) to the court in electronic format. Upon successful submission, a litigant can track the progress and status of his or her document in court. Information about the delivery of the document, its registration and other information are sent to the Electronic Cabinet of the author automatically. With the help of the E-court

service, a litigant can pay court fees and make other payments online, form and provide an electronic power of attorney to another person, and additionally receive: web links to the texts of all court-generated procedural documents in a case involving a party: court decisions, subpoenas, summonses, etc.; information on received and registered incoming documents on the case together with documents in electronic format; information on documents received in the case from other participants together with documents in electronic format; electronic documents that caused a change in the status of the case, automated distribution protocols, etc. (ELECTRONIC COURT…, 2020). However, the full implementation of the SJITS is a long process. Currently, only some courts have certain modules, and electronic lawsuits have to be duplicated on paper. This is caused by a number of problems, but with the government's active policy on digital transformation, one can expect rapid development in this area and further effective and transparent work of Ukrainian courts.

According to the Preamble to the Convention, fundamental human rights and freedoms are best ensured "through effective political democracy". In this regard, Article 3 of Protocol No. 1, which guarantees the mediation of freely elected representatives, as well as to vote and be elected in genuine periodic elections, which are held on the basis of universal and equal suffrage by secret ballot and ensure the freedom of expression of voters (PROTOCOL TO THE CONVENTION…, 1952). According to Article 25 of the International Covenant on Civil and Political Rights (1966) every citizen without any discrimination and without unreasonable restrictions must have the right and opportunity to participate in public affairs both directly and through elected representatives. The European Court of Human Rights has formulated a number of legal provisions for the application of this rule, noting that holding elections at reasonable intervals is essential for a truly democratic society, as the preservation of fundamental human rights and freedoms is based essentially on democracy. These conditions, according to the Court, include, in addition to freedom of expression, protected by Article 10 of the Convention, the principle of equality in the treatment of all citizens in the exercise of their right to vote (active suffrage) and the right to nominate oneself in elections (passive suffrage).

Regarding the use of AI technologies in the electoral process, it should be noted that in Ukraine these technologies are still under development and require legislation, although in many foreign countries AI is widely used, in particular for electronic voting and rapid processing of election results. To date, the electronic voting system has been introduced in many countries around the world: USA, Canada, Brazil, India, Belgium, Australia, Estonia, South Korea. In the UK, Germany, France, Spain, Portugal, Italy, Norway, Switzerland, Russia, Kazakhstan, Japan, China, experiments on its use are carried out (SAVCHUK, 2015). In general, electronic voting is the fixation of the voter's will use electronic technology, which includes the voting process and the process of automatic counting of votes using electronic devices and special software (KARAVAEV, 2020). For the Ukrainian electoral system, "electronic voting" is a completely new, unknown phenomenon, so it is necessary to understand its essential characteristics. Electronic voting covers several different types of voting. It covers

both the process of voting by electronic means and the process of automatic counting of votes using electronic devices and special software (YAROVA, 2017). The following types of electronic voting procedures are already used in the world: remote voting using Passport ID and the Internet; physical voting at polling stations with the help of electronic ballot boxes; voting by means of special digital terminals (BULLETIN OF…, 2013).

In Europe, voting equipment began to be used in the Netherlands in 1969. In the early 1990s, the country's Ministry of the Interior introduced electronic voting. In 2000, almost 90% of voters used DRE equipment. However, due to pressure from opponents, technology in the 2008 elections in the Netherlands returned to traditional paper ballots (REVISED EUROPEAN CHARTER…, 2015). In Estonia, electronic voting has been used in local elections since 2005 and in parliamentary elections since 2007, during which 30,275 citizens voted online without leaving their homes (KAMINSKA et al., 2008). In 2002, Estonia introduced electronic signatures, digital ID cards with a code and a microchip containing visual data on the card, as well as two digital certificates designed to verify the identity of the cardholder and provide digital signatures. Today, most potential voters have electronic cards (ELECTRONIC DEMOCRACY…, 2012). Information about meetings of local self-government bodies in Estonia is published in advance on the city website, and then there is an opportunity to follow its course in real time: which of the deputies voted for what, whose interests did they defend? There is complete information about each of the officials here and the possibility of feedback from each one. There is complete information on almost every step of the mayor's office on the city website, you can even trace how much, where, on what grounds the budget funds were transferred, to, for example, provide clerks with stationery (FENAZZI, 2013).

Ukraine is still taking the first steps towards the application of the electronic voting system. At the legislative level, a proper basis for this has not yet been created. The People's Deputy of Ukraine O. Tyshchenko submitted a draft resolution to the Verkhovna Rada of Ukraine on the introduction of "electronic voting", which should ensure transparency of interaction between the government and citizens of Ukraine (DRAFT LAW…, 2011), but so far the project has not been implemented. Since 2002, the Unified Information and Analytical System "Elections" has been functioning in one form or another in the Central Election Commission, designed to quickly determine the preliminary voting results (Yarova, 2017). The National Ministry of Digital Transformation has implemented a pilot project with PrivatBank Smart-ID. It is an identification by electronic signature, which is stored not on the chip, but on the phone card. In this way, each person can easily obtain a means of personal identification. This innovation is another step towards the introduction of an electronic voting system. But the signature on the smartphone is not sufficiently protected from hacker attacks.

In Ukraine, a system of "electronic appeals" has been successfully implemented since 2015, which allows the public to consult public authorities, file a complaint or a proposal. An e-petition is one of the tools of e-democracy.

According to the Law of Ukraine "On Citizens' Appeals", a petition is a special form of a collective appeal of citizens, proposals (comments), statements (petitions) and complaints set forth in writing or orally (LAW OF UKRAINE NO. 393/96-VR …, 1996). The first petition to reach the required number of votes was a petition from the Ukrainian Gun Owners Association, which requires legislative approval of the right of Ukrainian citizens to protection. During the processing of information about signatures, so-called "bots" were found, which tried to increase the number of signatures (SHIMKIV, 2015). Research shows that in 2018, more than 1,000 consultations were provided through electronic applications (DOROZHKO, 2018).

Observance and Protection of Human Rights in Ukraine in the Application of AI

Ukraine's accession to the Council of Europe, on the one hand, was a significant step of this state in the process of European integration, and on the other hand, it testified to Ukraine's acceptance of a number of international legal obligations, first of all, respect and protection of human rights. Prominent among the commitments made to the Council of Europe is the ratification by Ukraine of the Convention for the Protection of Human Rights and Fundamental Freedoms (1997) in 1997, recognizing the jurisdiction of the European Court of Human Rights. Issues related to the use of AI should be regulated in accordance with the norms of international treaties and conventions ratified by the majority of (European) states. In particular, in accordance with specialized international agreements in the field of AI development: the Council of Europe Convention on Cybercrime (2001), also known as the Budapest Convention; European ethical Charter on the use of AI in judicial systems and their environment, General Data Protection Regulation (WHAT IS THE GDPR…, 2020). Ukraine is already using the experience of leading European countries, in particular Estonia, and is moving towards the creation of e-Ukraine (NOTIFICATION ON HOLDING…, 2020). The Ministry of Digital Transformation of Ukraine has developed a Concept for the Development of AI in Ukraine. As Deputy Minister of Digital Transformation Our main goal is to promote the development of AI and its integration into economically important sectors (NOTIFICATION ON HOLDING…, 2020). In this way, we will increase the share of intellectually capacious products and significantly strengthen Ukraine's position on the world market. Particular attention will be paid to the use of AI in cybersecurity and defense. It is also very important to have the right balance between AI developed by third-party suppliers and national ones.

The concept, developed by the Ministry of Finance, provides for the development of human capital and an emphasis on the education of developers in the field of AI, the development of enterprises using AI, the active introduction of AI technologies in the public sector and major industries. It also stipulates the need to respect the right to privacy. The Ministry of Education and Science has already set up an expert committee on AI. In the last days of September this year, the Ministry of Education and Science presented the concept of the state in a

smartphone – the online platform "Action". According to the plan, by 2024, 100% of public services will be available to Ukrainians online (VORONKOV, 2019). For a long time, there was no legislation in Ukraine that would regulate the issue of security in both information and cyberspace. The first attempt to resolve this issue was the Draft Law of Ukraine "On the Principles of Information Security of Ukraine", which proposed a distinction between information and cybersecurity. Therefore, the main requirement is that the personal data collected must be sufficiently protected, personal data must be collected, used and provided with the knowledge and consent of the person, and the person must have access to personal data collected about him, including the ability to correct or delete incorrect data. Article 182 of the Criminal Code is provided for those who illegally collect, store, destroy and disseminate confidential information about a person (CRIMINAL CODE…, 2001). The penalty for such activities is from 8,500 to 17,000 hryvnias, and for repeated crimes – even imprisonment for a term of 3 to 5 years (KUTSENKO, 2017).

Compared to other crimes against a person, this article has a rather small percentage of court verdicts, except that punishment for imprisonment is provided exclusively for repeated acts. In general, the legislator provided a fairly lenient punishment with a relatively small amount of fine. This judgment becomes fair, especially considering that in Ukraine the violation of this article of the Criminal Code occurs, according to the analyzed data, mainly due to leaks to the general public (Internet) of personal data of bank customers, in second place: leaks of information from institutions that provide medical services. The right to protection of personal data and confidentiality is an old fundamental human right, which has gained new and special relevance with the spread and development of information technology. This right is guaranteed to us by the Law "On Personal Data Protection" (LAW OF UKRAINE NO. 2297-VI…, 2010). According to Article 5 of this law, the main subjects of general cybersecurity within the state are: The President of Ukraine, which coordinates activities in the field of cybersecurity as a component of national security of Ukraine is carried out by the President of Ukraine through the National Security and Defense Council of Ukraine; National Cyber Security Coordination Center as a working body of the National Security and Defense Council; Cabinet of Ministers of Ukraine. Entities that directly implement cybersecurity measures within their competence are:

– ministries and other central executive bodies;

– local state administrations;

– local governments;

– law enforcement, intelligence and counterintelligence bodies, subjects of operative-search activity;

– Armed Forces of Ukraine, other military formations formed in accordance with the law;

– National Bank of Ukraine;

– enterprises, institutions and organizations classified as critical infrastructure;

– business entities, citizens of Ukraine and associations of citizens, other persons carrying out activities and/or providing services related to national information resources, information electronic services, electronic transactions, electronic communications, information protection and cyber security.

In Ukraine, the function of personal data protection is entrusted to the Commissioner of the Verkhovna Rada of Ukraine for Human Rights or simply – the Ombudsman. A separate Department for Personal Data Protection was established within the Secretariat of the Commissioner of the Verkhovna Rada of Ukraine for Human Rights (PRAVDYCHENKO, 2019). The powers of the Commissioner, in accordance with Article 23 of the Law of Ukraine No. 2297-VI "On Personal Data Protection" (2010), include conducting inspections, issuing instructions to prevent or eliminate violations of legislation on personal data protection, providing recommendations on the practical application of legislation on personal data protection, drawing up protocols on bringing to administrative responsibility and sending them to court. In accordance with the competencies defined by law, the Commissioner is a mediator, not a punitive body and cannot directly impose sanctions. Based on the inspections, the decision to impose sanctions is made by the courts, which significantly slows down the process. At the same time, the speed of dissemination of information, including personal information, on the Internet is such that prompt response is essential to protect violated rights. Sometimes the Office of the Commissioner does react to violations very quickly, but unfortunately, he is not able to cover all the blatant violations. Therefore, it is necessary to improve the legislation of Ukraine in order to increase the effectiveness of legal regulation of social relations in this area of public life. Namely, making the necessary systemic changes in the article of the Constitution of Ukraine, the Criminal Code and other normative legal acts.

In particular, if we analyze the existing regulations, we can see that for violations of legislation in the field of personal data protection, Ukrainian legislation provides for fines, which can be called symbolic – up to two thousand non-taxable minimum incomes, i.e. 34 thousand hryvnias (CODE OF UKRAINE…, 1984). Such amounts are quite insignificant for large companies, and therefore can hardly be a deterrent. The above problems suggest that today Ukraine has insufficient control over violations in the field of information leakage. In authors` opinion, this is due to the fact that the legislation does not keep up with the development of this area, as many crimes provided for in the EU in Ukraine remain unarticulated, and therefore unresolved.

CONCLUSIONS

A significant problem from the use of AI technologies today is the violation of human rights in the field of protection of privacy of private data on the Internet and interference in private and private life. Confirmation of the existence of human rights threats in one form or another when using AI requires finding ways to overcome risks and threats to human rights and restore violated rights and threats, as well as the proper functioning of the human rights

mechanism as a subsystem of human rights and freedoms. It is important not to exaggerate the benefits of AI, to balance the benefits of AI technologies, such as accuracy and speed of decision-making, and ethics and empathy, qualities that only a person can have in making decisions. Therefore, the authors support the view that the final decision-making right should belong exclusively to the person, checking and controlling the work of AI. At stake as a result of the use of AI are human rights enshrined in international legal instruments, such as the right to respect for private and family life, freedom of expression, nondiscrimination, the right to freedom of movement, the right to free and fair elections, the right to fair trial.

In authors` opinion, it is necessary to create a global (mandatory) international legislation on the development and implementation of AI, in particular to prevent its non-legal, i.e. non-civilizational, use. In addition, governments and companies that use AI technology should be aware of the imperfections of the data on which the technology is based and take care to prevent discrimination and human rights violations. In Europe, countries need to pay attention to and take into account the Recommendations on AI developed by the European Commission and find a compromise approach to the use of AI. In Ukraine, it is necessary to regulate the activities in the field of AI, in accordance with international standards for the protection of human rights, to develop its own national strategy for the formation of principles of ethical, social and regulatory application of AI. The state must create such conditions under which the development of AI has not had a negative impact on national security and Ukraine's compliance with its obligations under international treaties and agreements.

REFERENCES

A definition of AI: Main capabilities and scientific disciplines High-Level Expert Group on AI. (2019). Available at https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

AI: what is it and how can an ordinary person use it? (2018). Available at https://trainmindpower.com/iskusstvennyj-intellekt/

ALEKSIUK, E. (2019). *Deep fake media reality*. Available at https://cedem.org.ua/articles/deep-fake/

AZMUK, N. (2019). AI in the process of work in the digital economy: new challenges and opportunities. *Donbass Economic Bulletin*, 3, 137-145.

BAY, G. (2019). Transformation of HR-technologies under the influence of digitalization of business processes. *Economics and Organization of Management*, 2, 93-101.

BRUCE, R.-L., STRONG, A., BIELER, K., PEABODY, J., HANLON, E., SINMAO, D., & BOCK, M. (1994). *Human development. Report 1994*. Oxford: Oxford University Press.

CHUBATYUK, YU. (2018). *AI in the service of modern politicum: Threats to democratic principles and the need for new standards*. Available at https://www.everest.ua/analytics/shtuchnyj-intelekt-na-sluzhbi-suchasnogo-politykumu-zagrozy-demokratychnym-prynczypam-i-neobhidnist-unovyh-standartah/

Code of Ukraine on administrative offenses. (1984). Available at https://zakon.rada.gov.ua/laws/show/80731-10#Text

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 on AI for Europe. (2018). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN

Convention for the Protection of Human Rights and Fundamental Freedoms. (1997). Available at https://zakon.rada.gov.ua/laws/show/995_004#Text

Convention on Cybercrime. (2001). Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

Coordinated Plan on Artificial Intelligence (COM (2018) 795 final). (2018). Available at https://ec.europa.eu/knowledge4policy/publication/coordinated-plan-artificial-intelligence-com2018-795-final_en

Criminal Code of Ukraine of April. (2001). Available at https://zakon.rada.gov.ua/laws/show/2341-14#Text

DE HARO, E. (2018). How the enlightenment ends: Philosophically, intellectually – in every way – human society is unprepared for the rise of AI. Available at https://www.theatlantic.com/magazine/archive/2018/06/henry-kissinger-ai-could-mean-the-end-of-human-history/559124/

DOROZHKO, E. (2018). *Electronic petitions in Ukraine*. Available at https://www.prostir.ua/?library=elektronni-petytsiji-vukrajini

Draft Law of Ukraine "On the Concept of Implementation of the Electronic Voting System in Ukraine". (2011). Available at https://ips.ligazakon.net/document/JF6OG00A

DVOROVY, M. (2020). *How the Ministry of Education and Science sees AI in Ukraine: Analysis of the concept of AI development*. Available at https://dslua.org/publications/yak-mintsyfry-bachyt-ai-v-ukraini-analiz-kontseptsii-rozvytku-shtuchnoho-intelektu/

Electronic court. (2020). Available at https://id.court.gov.ua/

Electronic democracy: Citizens and power. (2012). Available at http://imrussia.org/ru/society/330-edemocracy-citizens-and-the-state

Ethics guidelines for trustworthy AI. (2019). Available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

European Commission for the Efficiency of Justice (CEPEJ). (2018). Available at https://rm.coe.int/ethical-charter-en-for-publication-4-december-/16808f699c

European Group on Ethics in Science and New Technologies (EGE). (2016). Available at https://ec.europa.eu/info/research-and-innovation/strategy/support-policy-making/scientific-support-eu-policies/ege_en

European Parliament resolution with recommendations to the Commission on Civil Law Rules on Robotics. (2017). Available at https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html

European strategy on Artificial intelligence. (2020). Available at https://ec.europa.eu/digital-single-market/en/artificial-intelligence

Extreme automation and connectivity: The global, regional, and investment implications of the Fourth Industrial Revolution. (2016). Available at https://www.ip-watch.org/weblog/wp-content/uploads/2017/09/ubs-vierte-industrielle-revolution-2016-01-21.pdf

Facebook is late in protecting personal data. (2020). Available at https://www.ukrinform.ua/rubric-technology/2787837-facebookzapiznivsa-iz-zahistom-osobistih-danih-cukerberg.html

Facebook to be fined $5bn over Cambridge analytic scandal. (2019). Available at https://www.bbc.com/news/world-us-canada-48972327

FENAZZI, S. (2013). *Swiss direct democracy in the digital age*. Available at https://www.swissinfo.ch/rus

FILIPOVA, I. (2020). *Legal regulation of AI: teach*. Nizhny Novgorod: Nizhny Novgorod State University.

Forecast of the world economy until 2030E. (2018). Available at https://clck.ru/UKoXZ

FULEY, T. (2015). *Application of the case law of the European Court of Human Rights in the administration of justice*. Kyiv: OSCE Project Coordinator in Ukraine.

G20 Ministerial Statement on Trade and Digital Economy. (2019). Available at https://www.mofa.go.jp/files/000486596.pdf

Guidelines on AI and Data Protection. (2019). Available at https://rm.coe.int/guidelines-on-artificial-protection/168091f9d8

GURIEVA, M. (2019). *AI and "new discrimination": How do technologies affect human rights and life?* Available at https://inspired.com.ua/creative/technology/shtuchnyj-intelekt-ta-nova-dyskryminatsiya-yak-tehnologiyi-vplyvayut-na-prava-ta-zhyttyalyudyny/?fbclid=IwAR3LZx6g_KZFbelRP5BhHWEfb9XJ4ERSdRRZZAiREg5Rf5sG8IEn6xq7v7A

HRYTSIAK, N.V., & SOLOVYOV, S.G. (2013). *Electronic democracy as a mechanism of political interaction*. Kyiv: National Academy for Public Administration.

Industry 4.0. A policy brief from the Policy Learning Platform on Research and Innovation. (2019). Available at https://www.interregeurope.eu/fileadmin/user_upload/plp_uploads/policy_briefs/INDUSTRY_4.0_Policy_Brief.pdf

International Covenant on Civil and Political Rights. (1966). Available at https://zakon.rada.gov.ua/laws/show/995_043#Text

JAUME-PALASÍ, L., & SPIELKAMP, M. (2018). *Digital-Atlas Deutschland: Überblick über die Digitalisierung von Wirtschaft und Gesellschaft sowie von KMU, NGOs, Bildungseinrichtungen sowie der Zukunft der Arbeit in Deutschland*. Available at https://www.iwconsult.de/aktuelles/projekte/digital-atlas

KAMINSKA, T., KAMINSKY, A., & PASICHNYK, M. (2008). *Foreign experience of e-government implementation*. Kyiv: National Academy for Public Administration.

KARAVAEV, I. (2020). *Online elections in Ukraine: Realities and prospects.* Available at https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/vibori-onlayn-v-ukrayini-realiyi-ta-perspektivi.html

KARPENKO, O. (2017). *Alibaba CEO Jack Ma – on the economy of the future: "Stop hoping for production to create jobs"*. Available at https://ain.ua/2017/09/21/dzhek-ma-ob-ekonomike-budushhego/

KRAKOVETSKY, O. (2018). *Review of national strategies for the development of AI*. Available at https://clck.ru/UKoKZ

Künstliche Intelligenz nur auf Kosten der Menschenrechte? (2020). Available at https://www.wienerzeitung.at/verlagsbeilagen/digitale-republik/2055529-Kuenstliche-Intelligenz-nur-auf-Kosten-der-Menschenrechte.html

KUTSENKO, S. (2017). *Protection of personal and personal data on the Internet: problems of legislative regulation.* Available at https://ukrainepravo.com/scientific-thought/legal_analyst/zakhist-osobistikh-ta-personalnikh-danikh-v-interneti-problemi-zakonodavchogovregulyuvannya/?fbc

Law of Ukraine No. 2297-VI "On Personal Data Protection". (2010). Available at https://zakon.rada.gov.ua/laws/show/2297-17#Text

Law of Ukraine No. 254k/96 "On the Adoption of the Constitution of Ukraine and its Entry into Force". (1996). Available at http://search.ligazakon.ua/l_doc2.nsf/link1/Z960254.html

Law of Ukraine No. 393/96-VR "On Citizens' Appeals". (1996). Available at https://zakon.rada.gov.ua/laws/show/393/96%D0%B2%D1%80#Text

MARK, D.R., & GURCHETAN, S.G. (2014). *Making laws in a digital age*. Available at https://www.parliament.uk/ documents/speaker/digital

MILLER, J. (2018). *Can a machine have empathy?* Available at https://www.linkedin.com/pulse/can-machine-have-empathy-jason-miller

Montreal Declaration for the Responsible Development of AI Launched. (2018). Available at https://www.declarationmontreal-iaresponsable.com/la-declaration

MSI-AUT Committee of experts on Human Rights Dimensions of automated data processing and different forms of artificial intelligence. (2020). Available at https://www.coe.int/en/web/freedom-expression/msi-aut

New guidelines on Artificial intelligence and data protection. (2019). Available at https://www.coe.int/en/web/human-rights-rule-of-law/-/new-guidelines-on-artificial-intelligence-and-data-protection

Notification on holding a public discussion of the draft order of the Cabinet of Ministers of Ukraine "On approval of the Concept of AI development in Ukraine". (2020). Available at https://thedigital.gov.ua/regulations/povidomlennya-pro-provedennya-publichnogo-gromadskogo-obgovorennya-proyektu-rozporyadzhennya-kabinetu-ministriv-ukrayini-pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini

Order of the Cabinet of Ministers of Ukraine "On Approval of the Concept of Development of Artificial Intelligence in Ukraine". (2020). Available at https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220

Order of the Cabinet of Ministers of Ukraine No. 67 "On Approval of the Concept of Development of the Digital Economy and Society of Ukraine for 2018-2020 and Approval of the Action Plan for its Implementation". (2018). Available at https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

OSIPOV, G. (2001). AI: State of research and look into the future. *Artificial Intelligence News*, 1, 3-13.

Outcome Document: First version of a draft text of a Recommendation on the Ethics of Artificial Intelligence. (2020). Available at https://unesdoc.unesco.org/ark:/48223/pf0000373434

PARISER, E. (2011). *Beware online "filter bubbles".* Available at https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles/transcript?language=uk

PAVLYUK, O. (2019). *Elections on a smartphone. How social media and messengers influence politics?* Available at https://hromadske.ua/posts/vibori-v-smartfoni-yak-socialni-media-ta-mesendzheri-vplivayut-napolitiku?fbclid=iwar3yxikzfemzjegi09byrunqmqeke62ls5im1gh7wilqaxzfsp0awnwx9-s

PETRYSHYN, O.V., POGORILKO, V., & Prytyka, D. (Eds). (2003). *Scientific and practical commentary on the Constitution of Ukraine.* Available at https://jurisprudence.club/pravo-konstitutsionnoe/konstitutsiya-ukrajini-naukovo-praktichniy.html

PONOMARENKO, I.V. (2018). Practical aspects of application of innovative digital technologies in marketing activities. *Economic Bulletin of the National Technical University of Ukraine "Kyiv Polytechnic Institute"*, 15, 413-421.

PRAVDYCHENKO, A. (2019). *Personal data online: Problems of regulation and prospects of protection*. Available at https://cedem.org.ua/articles/personalni-dani-onlajn/

Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms. (1952). Available at https://zakon.rada.gov.ua/laws/show/994_535#Text

PYRMA, R. (2019). Political facets of digital citizenship. *Power*, 4, 69-78.

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. (2016). Available at https://eur-lex.europa.eu/eli/reg/2016/679/oj

RENTYUK, V. (2019a). Merging AI and the "Internet of Things". *Control Engineering Russia*, 2(80), 60-72.

RENTYUK, V. (2019b). Robots, artificial "intelligence" and us. How can we live together? Part 2. *Control Engineering Russia*, 4(82), 58-62.

Report on the Rule of Law. (2011). Available at https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2011)003rev-e

Report on the safety and liability aspects of AI, 2020 (Cm COM (2020) 64 final). (2020). Available at https://eur-lex.europa.eu/legalcontent/en/TXT/?qid=1593079180383&uri=CELEX:52020DC0064

Revised European Charter for the participation of young people in public life at local and regional level. (2015). Available at https://rm.coe.int/168071b58f

ROZGHON, O. (2020). AI as digital technology in the economic development of society: Economic and legal aspects. In: T. Nestorenko, M. Gawron-Lapuszek (Eds.), *Modern Technologies in the Development of Economy and Human Well-Being*. Katowice: Publishing House of University of Technology.

SAVCHUK, O. (2015). *Electronic election systems: voting procedures and material means. International experience*. Available at http://euinfocenter.rada.gov.ua/uploads/documents/28966.pdf

SHEMSHUCHENKO, V. (2020). *Artificial intelligence of justice*. Available at https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/

SHIMKIV, D. (2015). *Detected manipulation of signatures will not preclude consideration of the president's petition for weapons rights*. Available at https://www.5.ua/suspilstvo/shymkiv-vyiavleni-manipuliatsii-z-pidpysamy-ne-zashkodiat-rozghliadu-prezydentom-petytsii-pro-pravo-nazbroiu-92582.html

SOROKA, L. (2019). Legal framework and possible risks of using AI and space technologies. *Law and Suspension*, 6(2), 209-215.

SPITZER, M. (2014). *Anti-brain: Digital technologies and the brain*. Moscow: AST.

SUKHOTERIN, A.I., EREMINA, E.V., & KRUCHININA, S.A. (2018). Modern trends in the development of AI: Accumulated experience, problematic issues and prospects. *Information Technology Bulletin*, 4, 117-124.

UNESCO launches study on AI for Sustainable Development at IGF 2019. (2019). Available at https://en.unesco.org/news/unescolaunches-study-artificial-intelligence-sustainable-development-igf-2019

UNESCO unveils summary research on AI's implications on human rights at 40th Human Rights Council. (2019). Available at https://en.unesco.org/news/unesco-unveils-summary-research-ais-implications-human-rights-40th-human-rights-council

UNESCO's expert group revises the draft text of the Recommendation on the ethics of AI. (2020). Available at https://en.unesco.org/news/unescos-expert-group-revises-draft-text-recommendation-ethics-artificial-intelligence

VARAKINA, O. (2019). Permitting consequences. *Legal Practice*, 51(1147), 17-18.

VAULINA, F. (2019). *AI taught to write fake news*. Available at https://zn.ua/ukr/TECHNOLOGIES/shtuchniy-intelekt-navchilipisati-feykovi-novini-321845_.html

VORONKOV, O. (2019). *Will Ukraine be safe in a smartphone? Four steps of data protection*. Available at https://nv.ua/ukr/biz/experts/bezpeka-danih-ukrajinciv-derzhava-v-smartfoni-yak-ce-bude-pracyuvati-50049227.html

What is the GDPR, the EU's new data protection law? (2020). Available at: https//gdpr.eu/what-is-gdpr/

White paper "On Artificial Intelligence – A European approach to excellence and trust". (2020). Available at https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

YAROVA, A. (2017). *Electronic elections in Estonia: Experience for Ukraine*. Available at https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/16665/173-175.pdf?sequence=1&isAllowed=y

ZAGARIY, V.K., KOVALCHUK, T.G., & SINILNYK, V.V. (2019). Priority of digital economy development for Ukraine. *Priazovsky Economic Bulletin*, 2(13), 64-68.