УДК 004.8; 343.21

DOI: https://doi.org/10.21564/2311-9640.2023.19.281123

Mykola Karchevskyi,
Doctor of Law, Professor, Vice-rector of Luhansk State University of Internal Affairs named after E.O. Didorenko (Sievierodonetsk, Ukraine), Member of Ukrainian National Group of AIDP-IAPL;
Oleksandr Radutniy,
PhD in Law, Associate Professor (Docent) of the Criminal Law Department of the Yaroslav Mudryi National Law University (Kharkiv, Ukraine), Member of Ukrainian National Group of AIDP-IAPL

ARTIFICIAL INTELLIGENCE IN UKRAINIAN TRADITIONAL CATEGORIES OF CRIMINAL LAW

At the request of the International Association of Criminal Law (AIDP-IAPL, Association International de Droit Pénal – a non-governmental organization on criminal law, Paris, France) within the framework of the XXI International Congress of Criminal Law "Artificial Intelligence and Criminal Justice", a subgroup of the Ukrainian national group of AIDP-IAPL in two scientists prepared detailed answers to questions about ▪ definition and legal qualification of Artificial Intelligence system (legal definition of AI system in Ukrainian law, Ukrainian AI-based systems for predictive policing, legal definition of Machine Learning in Ukrainian law, legal personhood or legal capacity to the AI systems), ▪ existing criminal offences and criminalization (illegal act committed by, through or against an AI system; new offences related to designing, programming, developing, producing, functioning or making use of AI systems; crimes of mere conduct, commission and omission offences, consummate offence, crimes with intent, etc.; who can be considered the possible perpetrator and/or victim of the new AI offences e.g. producers / programmers / system engineers / developers / designers etc.; specific mental element of individual criminal liability, possibility for legal persons be held liable for AI crimes committed by any person acting individually or having a leading position within the legal person; criminal responsibility of the perpetrator or of the legal person in order to avoid the risk of over- criminalization if the AI systems are produced, used or put on the market for legal purposes, e.g. for scientific or research reason; whether reports or legal literature suggest the introduction of new criminal offences linked to AI systems; positive obligations for persons and/or legal person designing, developing, producing, testing, selling or distributing AI systems etc.), ▪ applicability of Traditional Criminal Law Categories (possibility for AI system considered as a "computer system" as defined by Article 1, lett. of Cybercrime Convention and or Article 2, lett. a) of Directive EU/2013/40; specific problems with respect to the

principle of legality; admissibility of analogy in order to criminalize illegal acts related to AI systems; joint-perpetrator or participant in the commission of the crime; forms of secondary liability applicable to AI-related crimes; state of mind (e.g. dolus) on the part of the human agent who designed / programmed / developed / produced / circulated / marketed / used the AI system; exact and concrete modus operandi of the AI system in committing the offence etc.), ▪ *adaptation of Traditional Criminal Law Categories and academic debate (principle of culpability nullum crimen sine culpa and mens rea; compliance with the principle of culpability when the output causing the harm generated by the intelligent machine is neither wanted nor predictable by the human agent; compliance with the principle of culpability when an AI system is intentionally used by a human agent as a tool but the AI system carried out an offence different from the one wanted by the human agent; criminal participation and attempted crimes; liability of legal persons; necessary adjustments of the legal principles on criminal liability of legal persons when they are involved in AI-related crimes; necessary adjustments of policies and preventive measures within private organizations in order to guarantee a correct and regular use of AI systems etc.),* ▪ *alternatives to criminalization and non-criminal sources.*

***Key words**: artificial intelligence, criminal liability, criminal law, criminal justice, criminal offense, Association International de Droit Pénal, qualification, machine learning, legal personality of artificial intelligence, legal capacity of artificial intelligence, criminalization, excessive criminalization, perpetrator, victim person, responsibility of legal entities, positive obligations, principle of legality, principle of culpability, analogy, state of mind (dolus) of human agent, nullum crimen sine culpa, mens rea.*

Lately the Ukrainian National Group of the International Association of Penal Law (AIDP-IAPL, Association International de Droit Pénal – a criminal law non-governmental organization located in Paris, France) received the task of preparing the report "Traditional Criminal Law Categories and AI: Crisis or Palingenesis?" for the International Colloquium of Section I (Criminal Law – general part) of the XXIth International Congress of Penal Law "Artificial Intelligence and Criminal Justice". The research in Section I was conducted by the authors of this article. The task consisted in answering pre-formulated questions. Some of them are offered to your attention in the following form. Due to the constant development of the legislation and the improvement of the scientific views of the authors, the given answers may be clarified.

I. Definition and legal qualification of Artificial Intelligence system.

1. Is there a legal definition of AI system in Ukrainian law? On September 20, 2000, the resolution of the Presidium of the High Attestation Commission of Ukraine № 13-08/9 included in the passport of the specialty "05.13.03 – systems and control processes" systems of intellectual decision support in conditions of uncertainty in the management of technological processes

and complexes. This resolution also approved the passport of the specialty "05.13.23 – systems and means of artificial intelligence" which includes Specialty formula: Systems and means of artificial intelligence – a branch of science that deals with theoretical research, development and application of algorithmic and software-hardware systems and complexes with elements of artificial intelligence and modelling of human intellectual activity.

On December 14, 2006, by the Resolution of the Presidium of the High Attestation Commission of Ukraine № 31-06 / 11, the methods of artificial intelligence in economics were included in the passport of the specialty "08.00.11 – Mathematical Methods, Models and Information Technologies in Economics".

According to the List of scientific specialties (order of the Ministry of Education and Science, Youth and Sports of Ukraine № 1057 of September 14, 2011) technical sciences were supplemented by the specialty "05.13.22 – systems and means of artificial intelligence".

On August 30, 2017, by order of the Cabinet of Ministers of Ukraine № 600-r technology of artificial intelligence and robotics was included in the List of critical technologies in the field of armaments and military equipment.

On October 18, 2017, the Government of Ukraine (Cabinet of Ministers of Ukraine) adopted Resolution № 980 "Some issues of determining medium-term priority areas of innovation activity at the sectoral level for 2017–2021" in Section 8 of which provided as follows: development and implementation of artificial intelligence systems, including ▪ new intelligent transport technologies (unmanned vehicles, traffic management and planning in the city); ▪ technologies, algorithms and software and hardware of intelligent services for household, medical, social purposes; ▪ intelligent military systems (soldiers of the future, mobile demining works, intelligent weapons control systems); ▪ intelligent control systems for autonomous robots and robotic systems; ▪ intelligent decision support systems in conditions of uncertainty; ▪ pattern recognition systems (technical vision, speech, etc.); ▪ intelligent web technologies, cloud computing.

It should be noted that these provisions remain only on paper and have not yet been fully implemented as of the end of 2021.

The decision of the Council of the National Bank of Ukraine № 9-rd of March 31, 2020 recommended the launch of a program with testing of artificial intelligence methods in forecasting work with nonlinear processes.

The order of the Cabinet of Ministers of Ukraine № 1175-r of September 29, 2021 for the period 2022–2025 in the field of medicine plans to develop systems to support clinical solutions, personalized medicine, telemedicine, systems for big data processing (Big Data), artificial intelligence – engineering processing, use and acquisition of new knowledge using the model and data of the electronic health care system and related systems.

On December 2, 2020, the order of the Cabinet of Ministers of Ukraine № 1556-r approved the "Concept for the development of artificial intelligence in

Ukraine". The terms are used in the following sense: artificial intelligence – an organized set of information technologies, using which it is possible to perform complex tasks by using a system of scientific research methods and algorithms for processing information obtained or independently created during work, as well as create and use their own knowledge bases, decision-making models, algorithms with information and identify ways to achieve the objectives; branch of artificial intelligence – the direction of activity in the field of information technologies which provides creation, introduction and use of technologies of artificial intelligence.

2. Is Ukraine using AI-based systems for predictive policing? Order of the Ministry of Justice of Ukraine № 3184/5 of 15.09.2020 regulates the use of the automated system "Cassandra" to assess the risks of criminal behaviour of convicts. This document amends other regulations, in particular, ▪ Instruction on the work of departments (groups, sectors, senior inspectors) of control over the execution of court decisions of penitentiary institutions and pre-trial detention centers (order of the Ministry of Justice of Ukraine of June 8, 2012 № 847/5), ▪ Procedure for compiling a pre-trial report (order of the Ministry of Justice of Ukraine of January 27, 2017 № 200/5), ▪ Procedure for the formation and maintenance of the Unified Register of Convicts and Detainees (Order of the Ministry of Justice of Ukraine of June 26, 2018 № 2023/5).

The Cassandra system on the basis of automated inference algorithms provides the formation of risk assessment of re-offending. The data required for risk assessment are entered by the registrar. Determining the degree of risk of recidivism (low, medium, high, very high) is carried out by the subsystem Cassandra automatically on the basis of the algorithm for calculating points and compliance with the amount of points to the established degrees of risk. The Cassandra provides a forecast of a person's re-offending, which is based on the use of machine learning and algorithms for automated conclusions (forecasts), based on the results of processing large structured data sets.

The forecast of a person's re-offending is formed for the purpose of research, comparing the results of the forecast with the result of risk assessment and improving the risk assessment system.

The Department of Artificial Intelligence of Kharkiv National University of Radio Electronics together with the Main Directorate of the National Police in Kharkiv region within the framework of the agreement on scientific and technical cooperation launched a project in the field of data mining based on modern neuro-fuzzy computational intelligence technologies.

The research results are implemented in the information-analytical complex "RICAS – Real-time intelligence crime analytics system" (http://ricas.org). It is a unique intelligent data analysis system that combines the basic and most modern methods and techniques of criminal analysis and real-time analytical search, which can significantly increase the efficiency and effectiveness of crime detection in hot pursuit, as well as previously unsolved crimes. RICAS allows you to perform the

following types of analysis: • crime pattern analysis, • general profile analysis, • analysis of a specific investigation (case analysis), • comparative analysis, • offender group analysis, • specific profile analysis, • investigation analysis.

3. Is there a different legal definition of Machine Learning in Ukrainian law? There is no legal definition of Machine Learning in the national legislation and case law (decisions of the European Court of Human Rights and the Constitutional Court of Ukraine). Meanwhile, in the information space there is a training course "Machine Learning" by Prometheus[1]. This course provides a broad view of the field of machine learning. Main topics of the course: The problem of learning. Training and testing. Generalization theory. Characteristic descriptions and types of quality functionality. Decision trees. Linear regression. Logistic regression. Support Vector Machines. Clustering and dimensionality reduction. Introduction to neural networks. Learning without a teacher. Reinforced training. Modern libraries of machine learning.

The Machine Learning was developed within the framework of the Initiative for the Development of think tanks in Ukraine, implemented by the Renaissance Foundation in partnership with the Foundation for the Development of Analytical Centres (TTF) with the financial support of the Swedish Embassy in Ukraine. The views and opinions expressed in this course are those of the author and do not necessarily reflect the position of the Government of Sweden.

4. Does Ukrainian law confer legal personhood or legal capacity to the AI systems? The national legislation of Ukraine currently does not confer legal personhood or legal capacity to the AI systems. In the process of working on the new Criminal Code of Ukraine, the authors of the report were part of an advisory group to prepare a section on crimes against information security. The position of the advisory group was discussed at the International Scientific Conference "Special Part of the Criminal Code of Ukraine: System and Content", October 20–22, 2021.

According to M. V. Karchevskyi[2], a specific requirement for the provisions of criminal law on crimes related to the use of new technologies should, not surprisingly, must be the technological neutrality. It is able to ensure the necessary stability of legislation in modern conditions of constant changes in technology. A striking example here is the current version of Part 3 of Article 190 of the

[1] Machine Learning / Prometheus, IRF: ML 101. URL: https://courses.prometheus.org.ua/courses/IRF/ML101/2016_T3/about.

[2] *Karchevskyi, Mykola* (2012) "Kriminalno-pravova okhorona informaziynoi bezpeki Ukraini" [Criminal law protection of information security of Ukraine] 2012 monografia / M V. Karchevskyi; MVS Ukraini, Luganskiy dergavniy universitet im. E. O, Didorenka [Ministry of Internal Affairs of Ukraine, Luhansk State University of Internal Affairs named after E.O. Didorenko]. Lugansk: RVV LDUVS im. E. O. Didorenko, 2012. p. 263 (in Ukrainian); *Karchevskyi, Mykola* (2016) "Perspektivnie zadachi ugolovnogo prava v kontekste razvitia robototekhniki" [Perspective tasks of criminal law in the context of the development of robotics] 2016 Sozialna funksia kriminalnogo prava: problemi naukovogo zabezpechennia, zakonotvorennia ta pravozastosuvannia: materiali mignarodnoi naukovo-praktichnoi konferensii 12–13 govtnya 2016 roku / redkol.: V. Y. Taziy, V. I. Borisov ta insh. Kh.: Pravo, 2016. [The social function of criminal law: problems of scientific support, law-making and law enforcement: materials of the international scientific and practical conference, October 12–13. 2016]. p.p. 109–113 (in Ukrainian).

Criminal Code of Ukraine (fraud with the use of computer technology). How fair is it to consider fraud committed through illegal operations with the use of electronic computers as a serious criminal offense (sanction of Part 3 of Article 190 of the Criminal Code of Ukraine provides for punishment up to 8 (!) years in prison)? At the time of the inclusion of this norm in the Criminal Code of Ukraine (20 years ago), the use of computer technology to commit fraud could indeed indicate an increased public danger of encroachment. The prevalence of e-commerce and remote banking systems was insignificant. They have been used by large businesses. Therefore, the provisions of Part 3 of Art. 190 of the Criminal Code of Ukraine quite clearly outlined the range of acts that could reasonably be considered as a particularly qualified type of fraud, close in degree of public danger to fraud on a large scale. However, the rapid pace of penetration of information technology in the financial sector has led to a qualitative change in this type of fraud. Law enforcement agencies record a significant number of such crimes related to the infliction of harm, which corresponds to the signs of simple or qualified fraud (Part 1, Part 2 of Article 190 of the Criminal Code of Ukraine). Whether it is possible to consider reasonable, namely the interpretation of the norm, criminal-legal assessment of such actions under Part 3 of Art. 190 of the Criminal Code of Ukraine? The question is rather rhetorical. In modern conditions, there is no reason to say that the use of electronic computers in the process of fraud so increases the level of public danger of the act.

This example clearly demonstrates the thesis that in the conditions of rapid expansion of the scope of new technologies, the provisions of the Criminal Code are "tied" to certain technological aspects, will quickly lose relevance. They will acquire the character of those that do not reflect the objective level of social relations. That is why the inclusion in the Criminal Code of such concepts as “artificial intelligence”, “neurointerface”, “nanotechnology”, “genetic engineering” etc., should be considered critically. The highest legislative body of Ukraine (Verkhovna Rada of Ukraine) currently has no such registered bills.

But O. E. Radutniy[3] does not rule out the possibility of recognizing super-artificial intelligence as a subject (persona) of legal relations, and therefore a subject (persona) of criminal offense. This prediction is based on important specific properties of super artificial intelligence: 1) the ability to think abstractly; 2) perception and recognition of all signals of the outside world; 3) obtaining most of the knowledge through training, as opposed to downloading the original data; 4) strategic thinking; 5) ability to deduction and induction, analysis and synthesis; 6) the ability to model the course of thoughts of the opponent; 7) the ability to

[3] *Radutniy, Oleksandr* (2017) “Criminal liability of the Artificial Intelligence” [2017] Problems of legality. 2017. Issue 138. http://plaw.nlu.edu.ua/article/view/105661/106117; *Radutniy, Oleksandr* (2017) “Artificial Intelligence (shtuchniy intelekt) yak subektbpravovidnosin v galuzi kriminalnogo prava [Artificial Intelligence as a Subject of Legal Relations in the Field of Criminal Law].” U Politika v sferi borotbi zi zlochinnistu: Mizhnarodna naukovo-praktychna konferentsiia [International Scientific and Practical Conference “Policy on the Fight against Crime”]. Ivano-Frankivsk, 2017 (in Ukrainian); *Radutniy, Oleksandr* (2017) “Kriminalna vidpovidalnist shtuchnogo intelektu [Criminal Liability of Artificial Intelligence].” Informaziya i pravo 2 (2017): 124–33 (in Ukrainian).

work effectively in conditions of uncertainty and probability; 8) use of available information in the most expedient and optimal way, etc. But the main and defining features are the following: 1) awareness of the principles of their work and thus the ability to self-improvement (the first version forms an improved version of itself and so rewrites the program to infinity); 2) self-copying (ability to spread and self-preservation); 3) solving the problem by brainstorming with the involvement of many copies of himself; 4) the ability to make decisions and act independently of human, and so on. However, the recognition of artificial intelligence as a subject (persona) of crime and legal relations will be expedient and justified only if the entire legal system is reformatted, including criminal law. Therefore, along with Section XIV-1 "Measures of a criminal nature against legal entities" of the Criminal Code of Ukraine, the possibility of a conditional section XIV-2 under the conditional title "Measures of a criminal nature against electronic persona (identity)" is not excluded (Radutniy, 2018)[4].

II. Existing criminal offences and criminalization.

1. Have traditional offences and/or cybercrimes already been applied to illegal act committed by, through or against an AI system? The Unified State Register of Judgments of Ukraine (https://reyestr.court.gov.ua/) contains a small number of judgments that mention artificial intelligence, in particular:

• court decision of the Uzhhorod City District Court of the Zakarpattia Region of July 20, 2021 in case № 308/7867/21 – the level of danger to society of a person who has committed a criminal offense is determined by the automated system with artificial intelligence "Cassandra";

• court decision of the District Administrative Court of Kyiv in the case № 640/20662/18 of July 1, 2020-on the error of the tax authority in calculating the debt to the taxpayer, which occurred using a computer program with partial participation of artificial intelligence;

• court decision of the Leninsky District Court of Kharkiv of August 25, 2021 in the case № 642/6961/19 – the use by the media of a news aggregator to cover the information picture of the day;

• court decision of the Commercial Court of Kharkiv region of May 28, 2020 in the case № 922/4148/19 – Innovative artificial intelligence company "Roofstreet", for which the team Code&Care developed their product;

• court decision of the investigating judge of the Pechersk District Court of Kyiv of April 21, 2021 in case № 757/21307/21-k – pre-trial investigation established that a citizen of the People's Republic of China Person_1, who is the

[4] *Radutniy, Oleksandr* (2018) "Dodatkovi argumenti shodo pravosubeknosti shtuchnogo intelektu [Additional arguments on the legal personality of artificial intelligence]." In Internet rechey: problem pravovogo reguluvannya ta vprovadgennya: Mizhnarodna naukovo-praktychna konferentsiia [Internet of Things: Problems of Legal Regulation and Implementation], 46–50. Kyiv: Politekhnika, 2018 (in Ukrainian); *Radutniy, Oleksandr* (2018) "Mistze shtuchnogo intelektu v strukturi suspilnih vidnosin yaki ohoronyautsa kriminalnim pravom [The location of Artificial Intelligence in the Structure of Public Relations, which is Protected by Criminal Law]." In Fundamentalni problem kriminalnoi vidpovidalnosti: Naukoviy Polilog [Fundamental Problems of Criminal Liability: Scientific Polilog]. Kharkiv: Pravo 2018 (in Ukrainian).

director of Golden Eg Technology, since the beginning of 2018 began to show considerable interest in projects, including those with limited access, in the field of nanotechnology, artificial intelligence, medical engineering, heat;

• court decision of the Kyiv Court of Appeal of August 18, 2021 in the case № 757/37395/21-k – the equipment seized during the search is used by MMI Engineering LLC within the main activities of the company, namely: AI (training of artificial intelligence; computer programming), maintenance of computer networks and other activities. This equipment has nothing to do with cryptocurrency mining.

In these court decisions, artificial intelligence acts as • the subject of the criminal offense (case № № 757/21307/21-k on information with limited access to certain technologies); • innovative product (cases № 922/4148/19 and № 757/37395/21-k); • aggregator of news and analytical content (case № 642/6961/19); • a computer program in the service of the state – the tax authority (case № 640/20662/18) or the probation authority (case № 308/7867/21).

In addition, in the judicial practice of Ukraine (see https://reyestr.court.gov.ua/Review/97444075 or -/87299694) there are cases when certain algorithmic bots are used in criminal offenses in the field of trafficking in narcotic drugs, psychotropic substances, their analogues or precursors. In particular, this applies to cases of creating a bot in the Telegram channel for the automatic sale of psychotropic substances and drugs on the Internet. In these cases, criminal offenses were committed with the help of an appropriate computer program with elements of artificial intelligence. Thus, the Telegram chatbot, according to pre-settings, automatically generated information for the buyer about the place, method of payment, type and amount of drugs, psychotropic substances that the buyer wanted to get (case № 686/8319/20 from the Common Register of Judgments of Ukraine).

However, there is currently an active fight against such chatbots, in particular, due to the alternative chatbot “StopNarcotics” in the system of the National Police of Ukraine. With its help 1583 addresses were blocked. Police have also launched a special bot called “DrugHunters”, which can be used to anonymously report about drug or drug dealers.

2. Has Ukrainian law introduced new offences related to designing, programming, developing, producing, functioning or making use of AI systems? The national legislation of Ukraine does not have any new corpus delicti that would explicitly mention AI. The so-called “computer crimes” (in the narrow sense) are provided for in Section XVI of the Criminal Code of Ukraine (Articles 361–363-1). The main statistical indicators of this group of crimes for the last 5 years (2016–2020) are the following: the number of recorded criminal proceedings (registered crimes) increased from 865 (2016) to 2498 (2020); the number of convicts increased from 24 (2016) to 56 (2020). The vast majority of persons were convicted of unauthorized interference with computer equipment (Article 361 of the Criminal Code of Ukraine) and illegal actions of persons entitled to access

information (Article 362 of the Criminal Code of Ukraine). Starting from 2018, the number of convicted persons for selling or distributing malicious software or hardware (Article 361-1 of the Criminal Code of Ukraine) and information with limited access (Article 361-2 of the Criminal Code of Ukraine) is growing.

The national legislation of Ukraine does not have any new corpus delicti that would explicitly mention AI.

To date, there is no normative basis for recognizing AI as a subject of crime. According to the first part of Article 18 of the Criminal Code of Ukraine, the subject of a criminal offense is only a human sanity person who has committed a criminal offense at an age from which, in accordance with this Code, criminal liability may arise.

According to national legal doctrine, the AI system can be considered the object of a crime when it is part of the protected social relations, any AI system refers to methods or means of committing a crime.

3. Highlight whether they are crimes of mere conduct, commission and omission offences, consummate offence, crimes with intent, etc. According to Article 13 of the Criminal Code of Ukraine, a completed criminal offense is an act that contains all the elements of a criminal offense under the relevant article of the Special Part of this Code. An unfinished criminal offense is preparation for a criminal offense and attempt to commit a criminal offense.

According to Article 14 of the Criminal Code of Ukraine, preparation for a criminal offense is the search for or adaptation of means or tools, search for accomplices or conspiracy to commit a criminal offense, removal of obstacles, and other intentional creation of conditions for committing a criminal offense. Preparation for a criminal offense or a crime for which the article of the Special Part of this Code provides for imprisonment for up to two years or other, less severe punishment, does not entail criminal liability.

According to Article 15 of the Criminal Code of Ukraine, an attempt to commit a criminal offense is the commission by a person of direct intent of an act (action or omission) directly aimed at committing a criminal offense under the relevant article of the Special Part of this Code, if the criminal offense reasons that did not depend on her will. An attempt to commit a criminal offense is complete if the person has taken all the actions he or she deems necessary to complete the criminal offense, but the criminal offense has not been completed for reasons beyond his or her control. An attempt to commit a criminal offense is incomplete if the person, for reasons beyond his control, has not taken all the actions he considered necessary to bring the criminal offense to an end.

According to Article 24 of the Criminal Code of Ukraine, intent is divided into direct and indirect. Direct intent is if a person was aware of the socially dangerous nature of his action (action or inaction), foresaw its socially dangerous consequences and wanted them to occur. Indirect intent is if a person was aware of the socially dangerous nature of his action (action or inaction), foresaw its socially

dangerous consequences and although he did not want to, but consciously assumed their occurrence.

According to Article 25 of the Criminal Code of Ukraine, negligence is divided into criminal illegal self-confidence and criminal illegal negligence. Carelessness is a criminal illegal self-confidence if a person foresaw the possibility of socially dangerous consequences of his action (action or inaction), but recklessly hoped to prevent them. Carelessness is a criminal unlawful negligence if a person did not foresee the possibility of socially dangerous consequences of his action (action or inaction), although he should and could have foreseen them.

4. **Specify who can be considered the possible perpetrator and / or victim of the new AI offences (e.g. producers / programmers / system engineers / developers / designers etc.).** As long as the AI is not endowed with self-improvement properties and does not make decisions autonomously from humans, it is possible to consider the developer or user as the perpetrator of the crime. The victims of these crimes are not fundamentally different from the victims of traditional crimes.

5. Indicate whether individual criminal liability requires a specific mental element and whether it involves also recklessness and / or negligence. According to Article 24 of the Criminal Code of Ukraine, intent is divided into direct and indirect. Direct intent is if a person was aware of the socially dangerous nature of his action (action or inaction), foresaw its socially dangerous consequences and wanted them to occur. Indirect intent is if a person was aware of the socially dangerous nature of his action (action or inaction), foresaw its socially dangerous consequences and although he did not want to, but consciously assumed their occurrence.

According to Article 25 of the Criminal Code of Ukraine, negligence is divided into criminal illegal self-confidence and criminal illegal negligence. Carelessness is a criminal illegal self-confidence if a person foresaw the possibility of socially dangerous consequences of his action (action or inaction), but recklessly hoped to prevent them. Carelessness is a criminal unlawful negligence if a person did not foresee the possibility of socially dangerous consequences of his action (action or inaction), although he should and could have foreseen them.

6. Could the legal persons be held liable for AI crimes committed by any person acting individually or having a leading position within the legal person? According to the Criminal Code of Ukraine, a legal entity is not a subject (persona) of a crime, accordingly, it cannot bear legal responsibility. But with regard to legal entities, the Criminal Code of Ukraine contains Section XIV-1 “Measures of a criminal nature against legal entities”.

7. Indicate whether there is any defence excluding the criminal responsibility of the perpetrator or of the legal person in order to avoid the risk of over- criminalization if the AI systems are produced, used or put on the market for legal purposes, e.g. for scientific or research reason. Today, the liability of the executor or legal entity in AI matters is resolved in a general way on

the basis of traditional norms. In the process of working on the new Criminal Code of Ukraine, the authors of the report were part of an advisory group to prepare a section on crimes against information security. The position of the advisory group was discussed at the International Scientific Conference "Special Part of the Criminal Code of Ukraine: System and Content", October 20–22, 2021.

According to M. V. Karchevskyi[5], a specific requirement for the provisions of criminal law on crimes related to the use of new technologies should, not surprisingly, must be the technological neutrality. It is able to ensure the necessary stability of legislation in modern conditions of constant changes in technology.

8. Whether reports or legal literature suggest the introduction of new criminal offences linked to AI systems (please provide also bibliographic references). Today, it is clear that strong artificial intelligence is a hypothetical technology and will remain at this stage indefinitely. It is possible that technologies of strong artificial intelligence will take the status of a subject (persona) of law, then new spheres of justice will appear. In addition to traditional justice, we can talk about the emergence of two new types, conditionally call them "mixed justice" and "artificial intelligence justice" (M. V. Karchevskyi, 2019)[6]. Mixed justice will include forms of resolving legal disputes between individuals, legal entities, society and businesses. The justice of artificial intelligence will include forms of resolving legal disputes between robots (or unit of artificial intelligence). In addition, the functioning of this system of justice will counteract the work that threatens social development and stability. Most likely, the human justice system will not be copied for artificial intelligence. Fundamentally different physical characteristics and needs require a priori to abandon this approach. At the same time, the creation of this system will be a necessary condition to provide humanity with the opportunity to control the development of social processes. Most likely, the justice of artificial intelligence will be created on the basis of robots. The physical and intellectual data of a human, obviously, will be insufficient for the effective functioning of this system of justice. The creation of such a system will require generalization into clear algorithms of experience gained during the existence of traditional justice. Such a generalization may become one of the main directions of future legal science.

It is likely that changes in the judiciary will take place in a different scenario. For now, it is obvious only that the impact of strong artificial intelligence technologies on the fight against crime can be studied only hypothetically.

[5] *Karchevskyi, Mykola* (2018) "Pravove reguluvannya sozializazii shtuchnogo intelektu" [Legal regulation of socialization of artificial intelligence] 2017. 2(78) Visnik Luganskogo dergavnogo universitety im. E. O. Didorenka [Bulletin of Luhansk State University of Internal Affairs named after E. O. Didorenko]. 99-108 (in Ukrainian).

[6] *Karchevskyi, Mykola* (2019) "Perspektivi pravovogo reguluvannya v konteksti gipotezi rozvitku tekhnologiy transgumanizmu" [Perspectives of legal regulation in the context of the hypothesis of the development of transhumanism technologies] 2019. 1(87) Visnik Luganskogo dergavnogo universitety im. E O Didorenka [Bulletin of Luhansk State University of Internal Affairs named after E.O. Didorenko]. 115–127 (in Ukrainian).

At the same time, it makes sense today to consider the issue of compliance of the current criminal legislation with the level of artificial intelligence technologies only in the context of "weak" artificial intelligence, because it actually exists.

Taking into account the clarifications made, the answer to the question is "yes". The current Criminal Code of Ukraine is able to provide an adequate response to the consequences of the use of systems of "weak" artificial intelligence, is also able to provide adequate protection of rights and interests in the use of these technologies. To the draft of the new Criminal Code, O.E. Radutniy[7] proposed an article about illegal actions with the digital image of human persona.

9. Does your domestic law provide for positive obligations for persons and/or legal person designing, developing, producing, testing, selling or distributing AI systems? In general terms, such positive obligations are provided by the Order of the Cabinet of Ministers of Ukraine № 1556-r of December 2, 2020 "Concept of development of artificial intelligence in Ukraine".

The main task of state policy in the field of legal regulation of artificial intelligence is to protect the rights and freedoms of participants in relations in the field of artificial intelligence, development and use of artificial intelligence technologies in compliance with ethical standards.

In order to achieve the goal of the Concept in this area, the following tasks should be ensured: ▪ implementation of the norms enshrined in the "Recommendations on Artificial Intelligence" adopted in June 2019 by the Organization for Economic Cooperation and Development (OECD / LEGAL / 0449), subject to the ethical standards set out in Recommendations CM / Rec (2020) 1, approved 8 April 2020 by the Committee of Ministers of the Council of Europe for member states on the impact of algorithmic systems on human rights in the legislation of Ukraine; ▪ elaboration of the issue of compliance of the legislation of Ukraine with the guiding principles established by the Council of Europe on the development and use of artificial intelligence technologies and its harmonization with the European one; ▪ assessment of the possibility and determination of the limits (ethical, legal) of the use of artificial intelligence systems for the purposes of providing professional legal assistance; ▪ ensuring the functioning and operation of technical committees of standardization in accordance with the requirements of 7.1.5 DSTU 1.14: 2015 "National standardization. Procedures for the establishment, operation and termination of technical

[7] *Radutniy, Oleksandr* (2018) "Subyektnist shtuchnogo intelektu u kriminalnomu pravi [The Subjectivity of Artificial Intelligence in Criminal Law]." Pravo Ukraini 1 (2018): 123–36 (in Ukrainian); *Radutniy, Oleksandr* (2019) "Adaptation of criminal and civil law in view of scientific-technical progress (Artificial Intelligence, DAO and Digital Human Being)" [2019] Problems of Legality, No 144 (2019), [S.l.], n. 144, p. 138–152, March 2019. http://plaw.nlu.edu.ua/article/view/155819/159365; *Radutniy, Oleksandr* (2019) "Morality and Law for Artificial Intelligence" [2019] Proceedings of the 1st International Symposium on Intellectual Economics, Management and Education, September 20, 2019. Vilnius Gediminas Technical University. Vilnius: Vilnius Gediminas Technical University, 2019. p. 44–46.

committees of standardization "in the field of artificial intelligence; ▪ ensuring cooperation between the relevant Technical Committees of Ukraine and the international subcommittees of standardization ISO / IEC JTC 1 / SC 42 Artificial Intelligence on the joint development of standards in the field of artificial intelligence; ▪ support for initiatives to create organizational forms of cooperation between interested legal entities and individuals in the field of artificial intelligence; ▪ development of a Code of Ethics for artificial intelligence with the participation of a wide range of stakeholders.

III. Applicability of Traditional Criminal Law Categories.

1. According to Ukrainian law and / or jurisprudence, is the AI system considered as a "computer system" as defined by Article 1, lett. of Cybercrime Convention and / or Article 2, lett. a) of Directive EU/2013/40? On December 2, 2020, the order of the Cabinet of Ministers of Ukraine № 1556-r approved the "Concept for the development of artificial intelligence in Ukraine". In this Concept, the terms are used in the following sense: artificial intelligence – an organized set of information technologies, using which it is possible to perform complex tasks by using a system of scientific research methods and algorithms for processing information obtained or independently created during work, as well as create and use their own knowledge bases, decision-making models, algorithms with information and identify ways to achieve the objectives; branch of artificial intelligence – the direction of activity in the field of information technologies which provides creation, introduction and use of technologies of artificial intelligence.

2. Are there specific problems with respect to the principle of legality? Such problems do exist. However, they are not related to AI. They are caused in most cases by a distorted practice of applying the law, which at the level of the legal norm is formulated quite progressively and constructively in most cases. According to the Criminal Code of Ukraine "No one can be held responsible for acts that at the time of the commission were not recognized by law as an offense" (Part 2 of Article 58). The content of this principle is also disclosed in Part 2 of Art. 4 of the Criminal Code of Ukraine, according to which "the criminality and punishment of an act are determined by the law on criminal liability, which was in force at the time of the act". This provision, firstly, obliges public authorities and officials to strictly adhere to the rules of criminal law in prosecuting and punishing a person and, secondly, excludes the application of criminal law by analogy with actions that are not provided for norms of the General and Special Parts of the Criminal Code of Ukraine.

3. Is analogy admissible? Has it been used in order to criminalize illegal acts related to AI systems? The application of the law on criminal liability by analogy is prohibited by Part 4 of Art. 3 of the Criminal Code of Ukraine. A classic example is the prohibition of analogy in criminal law, as a result of which the composition of crimes cannot be established solely by judgment by analogy or other supplement to the rule of law (the principle of "nulla poena sine lege").

4. Are the provisions concerning attempted crime applicable to AI-related crimes? Are there already cases of AI-related crimes qualified as attempted crimes? According to the Criminal Code of Ukraine, the provision on attempted crime is applied to the subject (persona) of the crime in case of committing an act directly aimed at committing a crime, failure to complete the crime, the reasons for incompleteness of the crime do not depend on the will of the perpetrator. Today, artificial intelligence is not considered a subject (persona) of crime. Therefore, in all the above cases, artificial intelligence can be used as a tool or method of committing a crime.

5. Is it possible to apply existent rulings of joint-perpetration and participation in the commission of the crime to AI related crimes? Who can be considered a joint-perpetrator or participant in the commission of the crime (please refer to both human and artificial agents)? Is the ”**perpetration-by-another” liability model applicable?** According to the Criminal Code of Ukraine, complicity in a criminal offense is the intentional joint participation of several subjects of a criminal offense in the commission of an intentional criminal offense. AI is not the subject (persona) of a crime, so it cannot be an accomplice, perpetrator, organizer, instigator or accomplice.

6. Could legal persons be held criminally liable for AI-related crimes committed for their benefit in Ukrainian law? According to the Criminal Code of Ukraine, a legal entity is not a subject (persona) of a crime, accordingly, it cannot bear legal responsibility. But with regard to legal entities, the Criminal Code of Ukraine contains Section XIV-1 “Measures of a criminal nature against legal entities”.

7. Are forms of secondary liability applicable to AI-related crimes? At the level of legislation this issue is not resolved. According to the current legislation of Ukraine, legal entities are not subject (persona) to criminal liability. At the same time, as noted above, measures of criminal law may be applied to a legal entity. In addition to the grounds for the use of such measures in the Criminal Code of Ukraine, we consider it appropriate to provide for the possibility of their use if employees or officials of the legal entity committed in favour of the legal entity or third parties encroachment on privacy. In our opinion, with the further spread of artificial intelligence technologies, this segment of the relationship will be most vulnerable to abuse by legal entities.

8. Is the wording of existing offences (in particular, computer crimes and cybercrimes) capable of including illegal acts committed through or against an AI system? A comparative analysis of the Convention and the Criminal Code of Ukraine makes it possible to establish that most of the acts provided for in the Convention are recognized as crimes under Ukrainian law. Such acts include: illegal interception (Articles 163, 361, 362 of the Criminal Code of Ukraine); interference with data (Articles 361, 362 of the Criminal Code of Ukraine); interference in the system (Article 361 of the Criminal Code of Ukraine); crimes related to child pornography (Article 301 of the Criminal Code of Ukraine);

forgery related to computers (Articles 358, 366 of the Criminal Code of Ukraine); fraud related to computers (Part 3 of Article 190 of the Criminal Code of Ukraine). The acts provided for in the Additional Protocol to the Convention are covered by Art. 161 of the Criminal Code of Ukraine, which establishes liability for violation of equality of citizens depending on their race, nationality or religion, and the general rules of the Special Part of the Criminal Code of Ukraine, which provide for crimes against freedom of conscience (Articles 178–181 of the Criminal Code of Ukraine).

At the same time, national criminal law, unlike the Convention, does not provide for liability for such an act as intentional access to all or part of a computer system without any right.

Note that, like the distribution or sale of malicious software, illegal access cannot be considered an encroachment that poses an independent public danger. Therefore, in the process of discussing changes to the Criminal Code of Ukraine, a proposal was made to criminalize unauthorized access as a qualifying feature of encroachments on computer data[8].

National criminal law does not explicitly provide for liability for actions such as: 1) intentionally selling, distributing or otherwise providing for use computer passwords, access codes or similar data that can be used to access all or part of a computer system with the intention of using it to commit any of the crimes listed in Articles 2 to 5 of the Convention; 2) possession of devices, including computer programs designed or adapted primarily for the purpose of committing any of the offenses listed in Articles 2 to 5 of the Convention, or computer passwords, access codes or similar data by which access can be obtained to all or part of the computer system with the intention of using it to commit any of the offenses listed in Articles 2 to 5 of the Convention, with the intention of using these items to commit any of the offenses listed in Articles 2 to 5.

However, the existence in the national legislation of provisions on criminal liability of accomplices and definitions of such concepts as "preparation for a crime", "attempted crime" suggests that although these acts are not expressly provided by the Criminal Code, their legal assessment as crimes is possible[9].

The so-called "computer crimes" (in the narrow sense) are provided for in Section XVI of the Criminal Code of Ukraine (Articles 361–363-1). The main statistical indicators of this group of crimes for the last 5 years (2016–2020) are the following: the number of recorded criminal proceedings (registered crimes) increased from 865 (2016) to 2498 (2020); the number of convicts increased from 24 (2016) to 56 (2020). The vast majority of persons were convicted of unauthorized interference with computer equipment (Article 361 of the Criminal

[8] *Karchevskyi, Mykola* (2012) "Kriminalno-pravova okhorona informaziynoi bezpeki Ukraini" [Criminal law protection of information security of Ukraine] 2012 monografia / M. V. Karchevskyi; MVS Ukraini, Luganskiy dergavniy universitet im. E. O. Didorenka [Ministry of Internal Affairs of Ukraine, Luhansk State University of Internal Affairs named after E. O. Didorenko]. Lugansk: RVV LDUVS im. E.O. Didorenko, 2012. p. 263 (in Ukrainian).

[9] Ibid. p. 265.

Code of Ukraine) and illegal actions of persons entitled to access information (Article 362 of the Criminal Code of Ukraine). Starting from 2018, the number of convicted persons for selling or distributing malicious software or hardware (Article 361-1 of the Criminal Code of Ukraine) and information with limited access (Article 361-2 of the Criminal Code of Ukraine) is growing.

9. Clarify whether, for the purpose of criminal liability, the state of mind (e.g. dolus) on the part of the human agent who designed / programmed / developed / produced / circulated / marketed / used the AI system shall include the exact and concrete modus operandi of the AI system in committing the offence. According to the existing legal doctrine and norms of law, the subject of a crime (the person who designed, programmed, developed, manufactured, distributed, sold, used an AI system) must: 1) know the subject of the crime (the methods of operation of the artificial intelligence system) and through it know the object of the crime (those social relations which are infringed by the crime); 2) foresee, at least in general terms, probable or unavoidable consequences; 3) to directly wish the onset of such consequences (direct intent – Part 2 of Article 24 of the Criminal Code of Ukraine), or consciously allow their occurrence (indirect intent – Part 3 of Article 24 of the Criminal Code of Ukraine), or carelessly rely on their prevention (criminal arrogance – Part 2 of Article 25 of the Criminal Code of Ukraine); 4) did not foresee the possibility of the onset of such consequences although he or she was obliged to foresee them and to have such a possibility (criminal negligence – part 3 of article 25 of the Criminal Code of Ukraine).

10. Assuming that the crime is caused by the autonomous ”**conduct” of the AI system, could the person who designed / programmed / developed / produced / sold / used of the AI system be held criminally liable if he had knowledge of its autonomous learning and decision-making capacity?** In the case at hand, such a person should first of all warn all other subsequent consumers, for example, in a wrapper license, about the mentioned properties of the AI. In fact, this may remove subsequent liability. In the same case, if there is no warning, the developer or other person may be liable for the latent defects of his product.

11. Are there in your domestic legal system cases of criminal liability for negligent or reckless conducts which can be applied when a crime or an illegal result is caused by conduct consisting in programming, producing or making use of an AI system? Such cases can be described by the following normative formulas. Article 25 of the Criminal Code of Ukraine. Carelessness and its types. 1. Negligence is divided into criminal illegal self-confidence and criminal illegal negligence. 2. Negligence is a criminal illegal self-confidence, if a person foresaw the possibility of socially dangerous consequences of his action (action or inaction), but recklessly hoped to prevent them. 3. Negligence is a criminal unlawful negligence if a person did not foresee the possibility of socially dangerous consequences of his action (action or inaction), although he should and could have foreseen them.

As stated earlier, legal doctrine and legislation do not provide for corporate criminal liability and the criminal liability of legal persons. Any defects in the programming, creation, or updating of the AI system are just as important as similar defects in any other product, method, or service. Administrative, civil, or criminal liability may apply in individual cases.

In the area of IT regulation, there are no specific positive obligations, other than the usual ones for all goods and services. In terms of criminal law, the general standard of care and possible criminal liability is formulated as follows.

Article 227 of the Criminal Code of Ukraine. Deliberate introduction of dangerous products on the Ukrainian market (release on the Ukrainian market): Deliberate introduction into circulation (release on the market of Ukraine) of dangerous products, i.e. such products that do not meet the requirements for product safety established by regulations, if such actions are committed on a large scale – shall be punishable by a fine of 3,000 to 8,000 non-taxable minimum incomes of citizens with deprivation of the right to hold certain positions or engage in certain activities for up to three years. Note. The introduction into circulation (release on the market of Ukraine) of dangerous products made in large quantities should be considered the introduction into circulation of products whose total value exceeds five hundred non-taxable minimum incomes.

The current legislation of Ukraine does not provide for such forms of liability as secondary liability or indirect violation.

IV. Adaptation of Traditional Criminal Law Categories and academic debate.

1. With regard to cases involving AI systems in Ukraine, does the case law or the academic debate point out legal issues concerning the traditional categories of the general part of the criminal law? In the criminal law of Ukraine, the equivalent of the Actus reus is the concept of the objective side of the crime – all the external manifestations of a particular offense. In a broad sense, almost any crime can be committed with the use of AI. As mentioned above, at present AI cannot be recognized as the subject of a crime, i.e. the person who committed it. In the narrow sense, the following crimes can be committed with the use of AI.

Section XVI of Criminal Code of Ukraine "Criminal offenses in the field of use of computers (systems), systems and computer networks": ▪ Article 361. Unauthorized interference in the work of electronic computers (computers), automated systems, computer networks or telecommunication networks. ▪ Article 361-1. Creation for the use, distribution or sale of malicious software or hardware, as well as their distribution or sale. ▪ Article 361-2. Unauthorized sale or dissemination of restricted information stored in computers, automated systems, computer networks or on such media. ▪ Article 362. Unauthorized actions with the information which is processed in electronic computers (computers), automated systems, computer networks or stored on carriers of such information, made by the person having the right of access to it. ▪ Article 363. Violation of rules of operation

of electronic computers (computers), automated systems, computer networks or telecommunication networks or the order or rules of protection of the information which is processed in them. ▪ Article 363-1. Interference with the operation of computers, automated systems, computer networks or telecommunication networks through the mass dissemination of telecommunication messages.

O. E. Radutniy does not rule out the possibility of recognizing super-artificial intelligence as a subject (persona) of legal relations, and therefore a subject (persona) of criminal offense (see question 4 of section I)[10].

2. Principle of culpability (nullum crimen sine culpa) and mens rea. Compliance with the principle of culpability when the output causing the harm generated by the intelligent machine is neither wanted nor predictable by the human agent. Compliance with the principle of culpability when an AI system is intentionally used by a human agent as a tool but the AI system carried out an offence different from the one wanted by the human agent. When the result of harm generated by an intelligent machine is neither desirable nor foreseeable to a human being there is an act of innocent infliction on the part of the human being. In such a case, the person cannot be held criminally responsible. The situation under consideration points to the need to discuss the possibility of recognizing AI as a subject of crime.

Traditional criminal law asserts that a person can be held liable only for those acts which were covered by his consciousness. Even without reference to AI, such a case (going beyond the agreement between accomplices by one of them) is referred to as the "excess of the perpetrator". Thus, in accordance with Part 5 of Article 29 of the Criminal Code of Ukraine, accomplices are not subject to criminal liability for an act committed by the perpetrator, if it was not covered by their intent.

3. Criminal participation and attempted crimes. Could a human agent be liable for participation in a crime committed or for an harmful result caused by an AI systems or AA? Also for a crime different from the one intended by some of the participants, because of the autonomous and unpredictable functioning of the artificial agent (ii). End of the preparatory phase and starting of the phase of execution: which acts performed by an AI system or by AA can be considered as attempted crime? A human agent may be liable for a crime if he is responsible for the actions of the AI as an instrument, means, or method of performing certain acts. Based on the fact that the AI is not the subject of the crime, no action by the AI as preparation can be considered an attempted crime.

4. Liability of legal persons. Necessary adjustments of the legal principles on criminal liability of legal persons when they are involved in AI-related crimes. Necessary adjustments of policies and preventive measures within private organizations in order to guarantee a correct and regular use

[10] Radutniy O. Criminal liability of the Artificial Intelligence. *Problems of legality*. 2017. Issue 138. http://plaw.nlu.edu.ua/article/view/105661/106117.

of AI systems. According to the Criminal Code of Ukraine, a legal entity is not a subject (persona) of a crime, accordingly, it cannot bear legal responsibility. But with regard to legal entities, the Criminal Code of Ukraine contains Section XIV-1 "Measures of a criminal nature against legal entities". Article 96-3 of the Criminal Code of Ukraine. Grounds for applying criminal and legal measures to legal entities: 1. The grounds for applying to a legal entity measures of a criminal nature are: 1) commission by its authorized person on behalf and in the interests of a legal entity of any of the criminal offenses provided for in Articles 209 and 306, parts one and two of Article 368-3, parts one and two of Article 368-4, Articles 369 and 369-2 of this Code; 2) failure to ensure the fulfillment of obligations imposed on its authorized person by law or constituent documents of a legal entity to take measures to prevent corruption, which led to the commission of any of the criminal offenses provided for in Articles 209 and 306, parts one and two of Article 368-3, parts one and two of Articles 368-4, Articles 369 and 369-2 of this Code; 3) its commission by an authorized person on behalf of a legal entity of any of the criminal offenses provided for in Articles 258–258-5 of this Code; 4) its commission by an authorized person on behalf of and in the interests of a legal entity of any of the criminal offenses provided for in Articles 109, 110, 113, 146, 147, parts two to four of Article 159-1, Articles 160, 260, 262, 436, 437, 438, 442, 444, 447 of this Code; 5) the commission by its authorized person on behalf of and in the interests of a legal entity of any of the criminal offenses provided for in Articles 255, 343, 345, 347, 348, 349, 376–379, 386 of this Code; 6) the commission of any of the criminal offenses provided for in Articles 152–156-2, 301-2–303 of this Code by an authorized person on behalf of and in the interests of a legal entity in relation to a minor or a minor. Note 1. Authorized persons of a legal entity should be understood as officials of the legal entity, as well as other persons who, in accordance with the law, the constituent documents of the legal entity or the contract have the right to act on behalf of the legal entity. 2. Criminal offenses provided for in Articles 109, 110, 113, 146, 147, 152–156-1, parts two to four of Article 159-1, Articles 160, 209, 255, 260, 262, 301-1 -303, 306 , 343, 345, 347, 348, 349, parts one and two of Article 368-3, parts one and two of Article 368-4, Articles 369, 369-2, 376–379, 386, 436, 437, 438, 442, 444, 447 of this Code, are recognized as committed in the interests of a legal entity, if they led to its illegal benefit or created conditions for such benefit, or were aimed at evading liability under the law.

Article 96-4 of the Criminal Code of Ukraine. Legal entities to which measures of criminal law are applied: 1. Measures of a criminal law nature, in the cases provided for in paragraphs 1 and 2 of part one of Article 96-3 of this Code, may be applied by a court to an enterprise, institution or organization, except state bodies, authorities of the Autonomous Republic of Crimea, local governments, organizations established by them in the prescribed manner, which are fully supported by the state or local budgets, funds of compulsory state social insurance, the Deposit Guarantee Fund of individuals, as well as international organizations.

2. Measures of a criminal law nature, in the cases provided for in paragraphs 3–6 of part one of Article 96-3 of this Code, may be applied by a court to subjects of private and public law of residents and non-residents of Ukraine, including enterprises, institutions or organizations, state bodies, authorities of the Autonomous Republic of Crimea, local governments, organizations established by them in the prescribed manner, foundations, as well as international organizations, other legal entities established in accordance with the requirements of national or international law. If the state or state-owned entity has a stake of more than 25 percent in the legal entity or the legal entity is under the effective control of the state or state-owned entity, the legal entity is fully liable for wrongfully obtained gain and harm caused by criminal an offense committed by the state, subjects of state property or public administration. 3. In case of reorganization of legal entities specified in parts one and two of this article, measures of criminal law nature may be applied to their successors to whom property, rights and obligations related to the commission of criminal offenses referred to in paragraphs 1-6 of the first part of Article 96-3 of this Code.

V. Alternatives to criminalization and non-criminal sources.

1. Does Ukrainian law use civil and / or administrative sanctions (e.g. payment of damages, closing of enterprise, etc.) in order to fight abuses of AI systems or harm caused by them? According to Article 96-6 of the Criminal Code of Ukraine "Types of measures of a criminal law nature applicable to legal entities": 1. The following measures of a criminal law nature may be applied to legal entities by a court: 1) fine; 2) confiscation of property; 3) liquidation. 2. A fine and liquidation may be applied to legal entities only as the main measures of a criminal law nature, and confiscation of property – only as an additional one. When applying measures of a criminal law nature, a legal entity is obliged to reimburse the damages and damages in full, as well as the amount of illegal gain received, which was received or could have been received by the legal entity.

2. Is there any form of compulsory civil insurance for damages resulting from the use of an AI system? Compulsory civil insurance is provided for all sources of increased danger, which today can fully include AI.

3. Are there other technical means for combating harm and/or abuses of AI systems? (e.g. re-programming of the AI system software; destruction of the artificial agent; or similar)? Such technical means exist at the level of individual companies or institutions and are described by internal regulations, to which access is often restricted for security or secrecy reasons.

4. To what extent are users expected to protect themselves (e.g. through security measures in using AI systems; intervention obligations in case of danger, etc.)? What legal relevance could reasonable self-protection of users have in crimes related to AI systems? Could it be a defence for producers accused of an AI-related crime? The higher the level of understanding and technical capability, the higher the level of protection for each

individual user. However, any level of reasonable protection on the part of the user is no excuse for negligence or violation on the part of the manufacturer.

5. To what extent is the product liability legislation applicable to emerging AI employment? Is there a specific regulation for AI systems ' testing phase? Alternatively, does the law require simulation obligations? Product liability legislation is fully applicable to new AI systems. The corresponding article of the Criminal Code of Ukraine was cited earlier. Regulation of the testing phase takes place at the level of individual companies or institutions and is described by internal regulations, to which access is often restricted for security or secrecy reasons. The development of these regulations is discussed at numerous conferences and discussions.

Numerous scientific conferences are also held, in which the authors of this report take part, in particular, • IV Kharkiv International Legal Forum (September 23-25, 2020) – public discussion "Human Dignity and Gender Equality: Constitutional Metamorphoses" and panel discussion "Rome Statute of the International Criminal Court: Problems of Implementation to the National Legislation of Ukraine"; • V Kharkiv International Legal Forum (Panel Discussion "Protection of the Economy from the Impact of Organized Crime", September 20, 2021); • International Scientific Conference "Special Part of the Criminal Code of Ukraine: System and Content" (October 20–22, 2021, Kharkiv); • Round table "Fundamental problems of jurisprudence III. Limits of Law" (April 23–24, 2021, Kharkiv); • Online Roundtable on Hate Crimes (EUAM – European Union Advisory Mission, EUAM Field Office in Kharkiv, Kharkiv, 25.03.2021); • International scientific-practical conference "Social, legal and managerial aspects of health care development: problems, prospects, world experience" (Lloret de Mar, Spain, February 5, 2021); • on-line Forum "New Opportunities for Ukraine in the Age of Pandemics", Panel "Tools for Counteracting Biological Threats" presentation "Antifragility – Tempering Communities with Constant Challenges" April 2, 2020; • VII International Scientific and Practical Conference "Human and Artificial Intelligence: Dimensions of Philosophical Anthropology, Psychoanalysis, Art Therapy and Philosophical Journalism" (May 21, 2020, Kyiv), report "New general and legal culture of human, digital and artificial relations. Intelligence"; • International scientific-practical round table "Criminal law in the context of globalization of social processes: traditions and innovations" (May 15, 2020, Kharkiv) Research Institute of Crime named after Academician VV Stashys NAPRN of Ukraine with the report "COVID-19, microchip and criminal liability"; • Lviv Forum of Criminal Justice (September 17-18, 2020, Lviv) "Ukrainian model of criminal justice: wandering in the mirror", report "The core and the crowd in the digitalization of law"; • Scientific-practical seminar "The use of artificial intelligence technologies in combating crime" of Research Institute for the Study of Crime named after Academician V.V. Stashis of the National Academy of Legal Sciences of Ukraine (November 5, 2020, Kharkiv), • Scientific and practical conference "Crime and countering it in conditions of singularity: trends and

innovations" (Kharkiv, April 16, 2021), • International scientific conference "Special part of the Criminal Code of Ukraine: system and content" (Kharkiv, 20–22 October 2021), • VI international scientific and practical round table on the topic "Criminal legal protection of information security" (Kharkiv, May 12, 2022), • VIII (XXI) Lviv criminal justice forum "Ukrainian criminal justice in conditions of war" (Lviv, June 9–11, 2022), • International scientific conference "Criminal law of Ukraine in the face of modern and future challenges: what is it like and what should it be?" (Kharkiv, October 21-22, 2022), • Panel discussion "Problems of adapting the criminal legislation of Ukraine to the acquis communautaire of the European Union" of the VI Kharkiv International Legal Forum (Kharkiv, October 5, 2022), etc.

6. Are there rules or principles (privacy by design, by default, etc.) on cybersecurity and data protection relevant to criminal aspects related to the design / production / use / development of AI systems? Such principles exist at the level of individual companies or institutions and are described by internal regulations, to which access is often restricted for security or secrecy reasons.

7. What is the role of the human agent? What degree of control over the AI system is granted or required? At today's level of AI development, the human agent is fully responsible for the quality or actions of the AI. However, it must be recognized that more and more AI is beginning to make more and more independent decisions with which humans agree. We need to see the point at which most decisions will be made for humans and then the AI will reach a new level of control over humans.

8. Is there a standardization of technical rules for designers / programmers / developers / producers of AI systems (or is it in the process of being defined)? The standardization of technical rules for designers / programmers / developers / manufacturers of AI systems exists at the level of individual companies or institutions and is described by internal regulations, which are often restricted for security or secrecy reasons.

REFERENCES

1. Karchevskyi, M. (2012). Kriminalno-pravova okhorona informaziynoi bezpeki Ukraini" [Criminal law protection of information security of Ukraine]. Lugansk: RVV LDUVS im. E. O. Didorenko [in Ukrainian].

2. Karchevskyi, M. (2016). Perspektivnie zadachi ugolovnogo prava v kontekste razvitia robototekhniki [Perspective tasks of criminal law in the context of the development of robotics]. *Sozialna funksia kriminalnogo prava: problemi naukovogo zabezpechennia, zakonotvorennia ta pravozastosuvannia: materiali mignarodnoi naukovo-praktichnoi konf. [The social function of criminal law: problems of scientific support, law-making and law enforcement: materials of the international scientific and practical conference]* (12–13 October, 2016). Kharkiv: Pravo [in Ukrainian].

3. Karchevskyi, M. (2018). Pravove reguluvannya sozializazii shtuchnogo intelektu [Legal regulation of socialization of artificial intelligence]. *Visnik Luganskogo dergavnogo universitety im. E. O. Didorenka – Bulletin of Luhansk State University of Internal Affairs named after E. O. Didorenko,* 2(78), 99–108 [in Ukrainian].

4. Karchevskyi, M. (2019). Perspektivi pravovogo reguluvannya v konteksti gipotezi rozvitku tekhnologiy transgumanizmu [Perspectives of legal regulation in the context of the hypothesis of the development of transhumanism technologies]. *Visnik Luganskogo dergavnogo universitety im. E. O. Didorenka – Bulletin of Luhansk State University of Internal Affairs named after E. O. Didorenko*, 1(87), 115–127 [in Ukrainian].

5. Machine Learning / Prometheus, IRF: ML 101. URL: https://courses.prometheus.org.ua/courses/IRF/ML101/2016_T3/about.

6. Radutniy, O. (2017). Criminal liability of the Artificial Intelligence. *Problems of legality,* 138, 132–141. http://plaw.nlu.edu.ua/article/view/105661/106117.

7. Radutniy, O. (2017). Artificial Intelligence (shtuchniy intelekt) yak subektbpravovidnosin v galuzi kriminalnogo prava [Artificial Intelligence as a Subject of Legal Relations in the Field of Criminal Law]. *Politika v sferi borotbi zi zlochinnistu: Mizhnarodna naukovo-praktychna konferentsiia [International Scientific and Practical Conference "Policy on the Fight against Crime"].* Ivano-Frankivsk [in Ukrainian].

8. Radutniy, O. (2017). Kriminalna vidpovidalnist shtuchnogo intelektu [Criminal Liability of Artificial Intelligence]. *Informaziya i pravo*, 2, 124–133 [in Ukrainian].

9. Radutniy, O. (2018). Dodatkovi argumenti shodo pravosubeknosti shtuchnogo intelektu [Additional arguments on the legal personality of artificial intelligence]. *Internet rechey: problem pravovogo reguluvannya ta vprovadgennya: Mizhnarodna naukovo-praktychna konferentsiia [Internet of Things: Problems of Legal Regulation and Implementation]*, 46–50. Kyiv: Politekhnika [in Ukrainian].

10. Radutniy, O. (2018). Mistze shtuchnogo intelektu v strukturi suspilnih vidnosin yaki ohoronyautsa kriminalnim pravom [The location of Artificial Intelligence in the Structure of Public Relations, which is Protected by Criminal Law]. *Fundamentalni problem kriminalnoi vidpovidalnosti: Naukoviy Polilog [Fundamental Problems of Criminal Liability: Scientific Polilog]*. Kharkiv: Pravo [in Ukrainian].

11. Radutniy, O. (2018). Subyektnist shtuchnogo intelektu u kriminalnomu pravi [The Subjectivity of Artificial Intelligence in Criminal Law]. *Pravo Ukraini*, 1, 123–136 (in Ukrainian).

12. Radutniy, O. (2019). Adaptation of criminal and civil law in view of scientific-technical progress (Artificial Intelligence, DAO and Digital Human

Being). *Problems of Legality*, 144, 138–152. http://plaw.nlu.edu.ua/article/view/155819/159365.

13. Radutniy, O. (2019). Morality and Law for Artificial Intelligence" [2019] Proceedings of the 1st International Symposium on Intellectual Economics, Management and Education, September 20, 2019. Vilnius Gediminas Technical University. Vilnius: Vilnius Gediminas Technical University.

Карчевський М. В., Радутний О. Е. Штучний інтелект в традиційних категоріях кримінального права України

На прохання Міжнародної асоціації кримінального права (AIDP-IAPL, Association International de Droit Pénal – неурядової організації з кримінального права, Париж, Франція) у рамках XXI Міжнародного конгресу кримінального права «Штучний інтелект і кримінальне правосуддя» підгрупа Української національної групи AIDP-IAPL у складі двох науковців підготувала розгорнуті відповіді на питання щодо ▪ визначення та правової кваліфікації штучного інтелекту (юридичне визначення штучного інтелекту в українському законодавстві, огляд національних систем штучного інтелекту для інтелектуальної поліцейської діяльності, правове визначення машинного навчання в українському законодавстві, правосуб'єктність або правоздатність систем штучного інтелекту тощо), ▪ наявних кримінальних правопорушень та їх криміналізації (незаконні дії, вчинені системою штучного інтелекту за допомогою системи штучного інтелекту або проти неї; нові правопорушення, пов'язані з проєктуванням, програмуванням, розробкою, виробництвом, функціонуванням або використанням систем штучного інтелекту; злочини, пов'язані з простою поведінкою; персона виконавця та/або жертви нових правопорушень, зокрема, виробники / програмісти / системні інженери / розробники / дизайнери тощо; специфічний психічний елемент індивідуальної кримінальної відповідальності, можливість для юридичних осіб нести відповідальність за злочини зі штучним інтелектом, вчинені будь-якою особою, яка діє індивідуально або займає керівну посаду в юридичній особі; межі кримінальної відповідальності злочинця або юридичної особи з огляду на уникнення ризику надмірної криміналізації, якщо системи штучного інтелекту виробляються, використовуються або пропонуються на ринок для законних цілей, наприклад, для наукових або дослідницьких цілей; огляд звітів або юридичної літератури щодо пропозицій впровадження нових кримінальних злочинів, пов'язаних із системами штучного інтелекту; позитивні зобов'язання для осіб та/або юридичних осіб, які проєктують, розробляють, виробляють, тестують, продають або розповсюджують системи штучного інтелекту тощо), ▪ можливості застосування категорій традиційного кримінального права (доцільність розуміння системи штучного інтелекту як «комп'ютерної системи» згідно з положеннями статті 1 Конвенції про кіберзлочинність та/або пунктом «а» статті 2

Директиви EU/2013/40; специфічні проблеми дотримання принципу законності; допустимість аналогії для криміналізації протиправних дій, пов'язаних із системами штучного інтелекту; форми вторинної відповідальності до злочинів, пов'язаних із штучним інтелектом; стан розуму (наприклад, dolus) з боку агента-людини, який проєктував / запрограмував / розробив / виготовив / поширив / продав / використав систему штучного інтелекту; точний і конкретний спосіб дії системи штучного інтелекту при вчиненні правопорушення тощо), ▪ адаптації категорій традиційного кримінального права та наукових дебатів (принцип винності nullum crimen sine culpa і mens rea; його дотримання, коли суспільно небезпечний результат заподіяний розумною машиною, не є ані бажаним, ані передбачуваним для людини; відповідність принципу винної відповідальності, коли система штучного інтелекту навмисно використовується агентом-людиною як інструмент, але система штучного інтелекту вчинила злочин, відмінний від того, якого бажає агент-людина; необхідність коригування правових принципів кримінальної відповідальності юридичних осіб, якщо вони причетні до злочинів, пов'язаних із штучним інтелектом; необхідність коригування політики та превентивних заходів у приватних організаціях для гарантування правильного та регулярного використання систем штучного інтелекту тощо), ▪ альтернатив криміналізації та некримінальних джерел відповідальності.

***Ключові слова**: штучний інтелект, кримінальна відповідальність, кримінальне право, кримінальне правосуддя, кримінальне правопорушення, Association International de Droit Pénal, кваліфікація, машинне навчання, правосуб'єктність штучного інтелекту, правоздатність штучного інтелекту, криміналізація, надмірна криміналізація, виконавець, потерпіла особа, відповідальність юридичних осіб, позитивні зобов'язання, принцип законності, принцип винної відповідальності, аналогія, стан розуму (dolus) агента-людини, nullum crimen sine culpa, mens rea.*