DECODING THE EU ARTIFICIAL INTELLIGENCE ACT: AN ANALYSIS OF KEY CONCEPTS AND PROVISIONS

https://doi.org/10.47743/jopafl-2024-31-33

TATARU Ștefan Răzvan
Alexandru Ioan Cuza University of Iaşi, Faculty of Law
Iași, România
razvantataru@gmail.com

CREȚU Andreea-Cosmina
Alexandru Ioan Cuza University of Iaşi, Faculty of Law
Iași, România
ancosmina@gmail.com

Abstract: Artificial Intelligence (AI) is a contemporary phenomenon of vast scale, surpassing the uses and opportunities brought by the advent of the Internet, but which generates fundamental rights risks and legal challenges at an exponentially higher level. In the present study, we aim to explore the concept of artificial intelligence, the types of AI technologies, and the requirements for market introduction, with direct reference to the provisions of the new European Union AI Act. For a better understanding of the concept of Artificial Intelligence, we will classify AI systems considering the following criteria: the degree of risk, the algorithms used, the capabilities and functions, and the level of autonomy of the system. The paper highlights key aspects of AI Act regulation, focusing on high-risk and prohibited AI systems. Finally, the penalties for non-compliance with AI Act provisions are briefly outlined.
Keywords: artificial intelligence; AI act; AI regulation; high-risk AI system.

Introduction

The concept of Artificial Intelligence originated in 1956 at the Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI) conference but has really expanded since the beginning of the Big Data era (Moor J., 2006). The sheer volume and diversity of data available is 'feeding' AI systems which, together with Web 4.0 & Industry 4.0 technologies, are radically changing business processes and the way individuals relate to technology. AI technology has been successfully "adopted" by many industries and has now become a strategic imperative for any business that wants to grow and succeed in a dynamic and competitive market. The advancement of new technologies and the accessibility of these systems has led in recent years to the use of AI systems directly by citizens in their day-to-day lives. Applications based on AI systems such as Amazon Alexa, Google Gemini, ChatGPT, Midjourney or DALL-E are widely used by individuals of all ages in their personal or professional activities (Ungureanu C.T., Amironesei A.E., 2023). Undoubtedly, AI is a current phenomenon, of a scale that goes beyond the uses and opportunities brought by the advent of the Internet, but which generates fundamental rights risks and legal challenges at an exponentially higher level. In the following, we aim to explore the concept of artificial intelligence, the types of AI technologies and the requirements for market introduction, by direct reference to the provisions of the new European Union AI Act (Proposal for a Regulation of The European Parliament and of the

Council Laying Down Harmonised Rules on Artificial Intelligence - Artificial Intelligence Act, as approved by the European Parliament on March 13, 2024).

Artificial Intelligence: concept & essentials

AI is not a new technology - some AI systems have been around for decades, but advances in computer power, the availability of vast amounts of data and new types of software have facilitated the development of the technology in a short time, leading to major breakthroughs in the field. AI is used in many applications in everyday life, such as virtual assistance, medical diagnostics, machine translation, navigation tools, production quality control, natural disaster prediction, etc. The EU supports the development of AI technology, but it also recognizes its potential risks, so it encourages an ethical approach focused on protecting fundamental human rights. In fact, the European Union is among the first legislators in the world to try to implement a law on artificial intelligence (European Commission, 2020). The AI Act has the potential to set a global benchmark for AI regulation in other jurisdictions, similar to the way the GDPR has operated, thus promoting the European approach to technology regulation on the world stage.

AI is essentially a tool that allows computers to mimic certain human behaviours. AI systems function using statistical methods that enable them to evolve through experiential learning. AI can be general, i.e. it can replicate human thought, feelings, and interaction, being the least developed component, or it can be specific, i.e. it has the ability to solve specific tasks. AI offers many opportunities to facilitate people's professional activities, as it can perform complex equations in seconds, analyse legal documents or support artistic creative acts. However, AI-based systems may affect certain rights, such as the right to information privacy, as they rely heavily on the collection and use of large amounts of data and may generate, based on the social patterns analysed, certain discriminatory or prejudicial predictions. This has given rise to the need to design a legal framework to allow the development and evolution of these systems in accordance with the rights of all those involved in their progress, from developers, facilitators, and distributors to all users, professional or amateur.

AI systems are software systems (possibly also hardware) designed by humans to act in the physical or digital dimension through perceiving their environment by collecting data, interpreting this data, whether structured or unstructured, and processing the information extracted from it to select the optimal action to take to achieve the given goal. AI can either use symbolic rules or learn a numeric model and is also able to adapt its behaviour by analysing how the environment has been affected by its previous actions. According to art. 3 AI Act, an "artificial intelligence system" (AI system) is defined as "software that [...] can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with". In addition, the Regulation specifies the ways in which an AI system can be developed, listing machine learning techniques - supervised, unsupervised and reinforcement learning, logic and knowledge-based approaches and search and optimisation methods.

AI Systems classification

For a better understanding of the concept of Artificial Intelligence we will classify AI systems taking into account the following criteria: the degree of risk, the algorithms used, the capabilities and functions, and the level of autonomy of the system. If the first criterion is established by AI Act, the following ones are derived from scientific literature. At the same time, we will briefly present the types of AI systems implemented, such as Reactive machines and Limited memory machines, as well as future technologies in AI such as theory of mind & self-awareness.

AI Systems Risk-Classification

Based on the principle that the higher the risk, the stricter the rules, the EU AI Act divides AI systems into four categories: minimal or no risk, limited risk, high risk and unacceptable risk.

a) Minimal or no risk. Most AI systems are risk-free and can continue to be used without being affected in any way by the regulation (e.g. video games, spam filters).

b) Limited risk. AI systems that pose only limited risks will be subject to broad transparency obligations, such as disclosing that the system provides AI-generated content so that users can make informed decisions about its further use (e.g. generative AI, such as a chatbot).

c) High risk. A high-risk AI system is one that presents a significant potential for causing harm or negative consequences due to malfunction or incorrect decision-making. A wide range of high-risk AI systems will be authorised if they comply with the requirements and obligations imposed by the Regulation for obtaining access to the EU market (e.g. AI systems used in medical diagnostic systems or autonomous driving systems).

d) Unacceptable risk. For certain uses of AI, the risk is considered unacceptable, so these systems will be banned within the Union, as they present a clear interference with fundamental human rights and freedoms. Uses include cognitive-behavioural manipulation, predictive policing (use of predictive analytics and other analytical techniques by law enforcement to identify potential criminal activity), emotion recognition in the workplace and educational institutions, and social scoring (practices in which AI is used to open or restrict access to social benefits or to differentiate social treatment of a person based on a score derived from an assessment of their personal behaviours or attributes). Remote biometric identification systems such as facial recognition will also be banned, with some exceptions.

AI classification based on the type of algorithms used

AI algorithms are a set of instructions or rules that allow systems to learn, analyse data and make decisions based on this knowledge. Algorithms can perform tasks that normally require human intelligence to perform (e.g. pattern recognition, natural language understanding, problem-solving and decision-making). In training algorithms, the focus is on the quality of the data input, the values of its use and its testing, with the quantity of data input being less important in the process. Three major categories of algorithms are distinguished: supervised learning, unsupervised learning and semi-supervised or consolidation learning (Tabsharani F., 2023).

a) Supervised learning is a fundamental category of algorithms in which an AI model is trained on a set of specific input data, called training data that has a known label or outcome. The objective of the algorithm is to learn a function by which it can accurately

classify or draw new and unpredictable data. Supervised learning is widely used in tasks such as image classification (identifying objects in images), natural language processing (sentiment analysis of digital text - the process of analysing a text to determine whether the emotional tone of the message is positive, negative or neutral) and recommender systems (product or content suggestions).
b) Unsupervised learning represents another fundamental category of algorithms, different from supervised learning in that it processes input data that is not labelled and has no known outcome. The algorithm operates by extracting general rules from the data, by reducing data redundancy or by organising the data based on similarity. Unsupervised learning is applied in customer splitting (identifying groups of customers that have similar behaviours), anomaly detection (detecting unusual patterns in the data), and topic modelling (identifying central themes in input texts).
c) Semi-supervised or consolidation learning is a distinct approach in which an agent interacts with an environment to learn a sequence of actions, with the input being a mixture of labelled and unlabelled examples. The agent explores various actions, receives feedback in the form of rewards or penalties, and adjusts its decision-making process over time to optimize its long-term performance. Reinforcement learning is used in robotics, certain video games, automotive vehicles (training automated cars to navigate safely) and recommender systems (learning user preferences).
These three major categories of artificial intelligence algorithms provide a versatile toolset for tackling a wide range of problems, from predictive modelling to hidden pattern discovery, and enable optimal decision-making in complex environments.

AI Classification based on functionality and capabilities

Categories of AI based on their capability

Considering its learning processes and capabilities, AI can be classified into 'narrow intelligence', 'general artificial intelligence', and 'super-intelligence' types, showcasing the evolving capabilities of AI systems. These systems can execute precise tasks and simulate, or even surpass, human thought processes.

Categories of AI based on their functionality

Aren Hintze, a researcher and professor at Michigan State University, defines four main types of AI, based on their functionality, grouped into two categories, as they exist in real life or only in theory: Reactive machines, Limited memory, Theory of Mind and Self-awareness (Hintze A., 2016; Alzoubi, A.A., Al Aqeel, I., Alzoubi, H.M., 2024.).
Existing AI systems: Reactive machines and Limited memory machines
a) Reactive machines are AI systems that have no memory and are specific to a single task, meaning that an input of data always gives the same output. Machine learning models tend to be reactive systems because they take customer data, such as search or purchase history, and use it to generate recommendations. They involve the "super" type of learning as humans are not able to process huge amounts of data (e.g. a customer's entire Netflix history) to issue personalised recommendations. Reactive systems do not have the ability to predict future outcomes unless they have been given adequate information.
b) Limited memory machines are AI systems whose algorithm mimics the way human neurons work together, meaning that it gets smarter as it receives more training input. Deep learning algorithms facilitate natural language processing, image recognition and other

semi-supervised learning methods. Unlike reactive systems, limited-memory ones can monitor specific objects or situations at a given time, even from the past. After this step, observations are programmed into the AI. A classic example of a limited-memory AI system is the autonomous vehicle - driverless cars observe the speed, direction, and position of other cars in traffic, and this data helps the vehicle decide when to change lanes.
Future technologies: Theory of mind and Self-aware AI
c) AI Theory of mind, if it will be developed and implemented, has the potential to understand the world through the lens of people's thoughts and emotions. Human cognitive abilities are able to process how our behaviours affect others and conversely, how we are affected, which is the basis of human relationships. In the future, AI systems operating based on theory of mind may be able to understand a person's intentions and predict their behavioural reactions, essentially simulating an inter-human relationship.
d) Self-aware AI's aim would be to design systems that are aware of their existence. This model goes beyond the ability of a system operating on theory of mind, processing the understanding of emotions to be aware of themselves, their state and to be able to sense or predict the feelings of others. For example, "I'm hungry" becomes "I know I'm hungry" or "I want to eat lasagne because it's my favourite food".

AI classification based on the level of autonomy
Artificial intelligence systems can be categorized, depending on how they are implemented and used, in standalone AI systems and Integrated AI components.
a) Standalone AI systems or Independent AI systems are AI solutions that can operate independently and autonomously without being integrated into other products or applications. Standalone AI systems are capable of operating and making decisions autonomously, without human intervention. They use advanced machine learning algorithms to analyse data and evaluate experiences to adapt their functionality. The use of these types of systems is beneficial in terms of independence (autonomous systems can perform tasks without constant human supervision, allowing for increased efficiency), decision-making (they can make informed, real-time decisions and optimise outcomes) and reducing human error (independent systems increase accuracy and reliability in various areas such as manufacturing, healthcare, and transportation).
b) Integrated AI components or Product-integrated AI systems are integrated into other products or applications to add intelligent functionalities or to enhance their performance. Today, AI is no longer just a tool, but a partner capable of guiding users in performing professional or personal tasks. When not a stand-alone system, AI can operate as an assistant on different platforms. For example, Microsoft has shown how its AI-based Copilot feature will increase the productivity of its users by automating and assisting with tasks, documents, and information. In Designer, the new graphic design app developed by Microsoft 365, the company has introduced several AI features for creating visual elements, social media posts and more (Brue M., 2023).

EU regulation of artificial intelligence

1. AI Act and previous regulatory attempts
Artificial Intelligence is one of the emerging and disruptive technologies of the 21st century, with the ability to significantly influence the way people and businesses do

business. AI technologies are currently not regulated at an international or regional level. However, in 2019 the OECD Principles for Artificial Intelligence were adopted by 46 countries (38 OECD members and 8 others). The OECD Principles for Artificial Intelligence are a set of guidelines for the responsible development and use of AI technologies in different sectors and industries. The principles proposed by the OECD are based on values such as: a. Inclusive growth, sustainable development and well-being; b. Human-centered values and fairness; c. Transparency and explainability; d. Robustness, security and safety; e. Accountability. At regional level, the Council of Europe is setting up a Committee on Artificial Intelligence which proposes principles and ethical standards for AI (CAHAI, 2020; Council of Europe, 2020). Subsequently, within the CoE, the Committee on Artificial Intelligence is active, and by the end of 2023, it presented a proposal for a Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CAI, 2023). Given that AI technologies are not limited to the jurisdiction of a particular state and have the capacity to be used internationally, we consider it necessary to regulate these systems at international or regional level. At the European level, the Commission has proposed in 2021 the first legal framework on artificial intelligence, part of the EU Data Package (Halford C., Air C., Eastwood H., (2022); Ungureanu C.T., 2021). The regulation of AI systems is an important step in the EU Digital Strategy and the adoption of the AI Act could serve as a benchmark at an international level, similar to the regulation of personal data protection through GDPR.

The AI Act is a legislative proposal for harmonised rules on Artificial Intelligence which aims primarily to ensure that fundamental rights are respected by any AI system placed on the European market. It also represents an opportunity to stimulate investment and innovation in this field by increasing safety for users of AI software. In parallel to the debate and adoption of the AI Act, the European Commission is working on a proposal for a Directive on the adaptation of non-contractual liability rules to artificial intelligence (AI Liability Directive). The risks associated with the use of new technologies act as a barrier to the rapid adoption of Artificial Intelligence, in any form or algorithm and regardless of the severity of the applicable regulations. What makes users trust AI? Can we assess an AI system as "trustworthy"?

According to the High-Level Expert Group on Artificial Intelligence, for an AI programme to be considered "trustworthy", it must encompass three essential components: it must be legal (compliant with all related regulations), ethical (ensures compliance with ethical values and principles) and robust (contains a broad technical component harmonised with the social environment, ensuring the safe and secure operation of the system and preventing any unintended negative impact) (High-Level Expert Group on Artificial Intelligence, 2019).

From an ethical point of view, a reliable AI system must be developed, implemented and used in a way that respects user autonomy and prevents harm, and takes into account the principle of fairness, with special attention to vulnerable users (children, people with disabilities, people belonging to disadvantaged groups). These requirements must be implemented and met throughout the system's operation, but the potential tensions between them may differ from application to application, depending on the domain or industry in which AI is used. While most requirements apply to all AI systems, particular attention should be paid to those that affect individuals directly or indirectly. In line with the first component of reliable AI - legality, developers and implementing organisations of AI

systems have a responsibility to ensure that legal obligations are met, both in terms of horizontally applicable rules and domain-specific regulations. With the entry into force of the AI Act, these obligations will be even easier to find, understand and enforce.

2. The risk-based approach

The AI Act proposes a clear division between acceptable and unacceptable risks, consequently determining trustworthy and untrustworthy AI (Laux J., Wachter S., Mittelstadt B. 2024).

Considering our above analysis of the categorization of AI based on risk levels, as outlined in the AI Act, we will now focus solely on high-risk AI and prohibited AI. The AI Act provides for a horizontal level of protection by classifying AI instruments into high-risk systems to highlight that those likely to cause serious violations of fundamental rights or other significant risks are targeted. Those that are classified as limited risk systems will be subject to less restrictive transparency obligations, e.g. disclosure of the use of such a system in creative content products ("content was generated by AI"), so that users are informed and can make informed decisions about that content.

High-risk AI systems will be able to gain access to the EU market if they comply with certain requirements and obligations to obtain authorisation, such as data quality and safety aspects.

High-risk AI systems: approval before marketing

As for high-risk systems, they will be able to gain access to the EU market if they comply with certain requirements and obligations in order to obtain authorisation, such as the implementation of risk assessment modalities, ensuring data quality and security, the preparation of comprehensive technical documentation and compliance with the transparency obligation.

Thus, the regulation provides for the need to establish, implement and maintain a risk management system, i.e. an iterative process that needs to be regularly and constantly updated throughout the lifetime of a high-risk AI system and that must go through the following steps:

(a) identifies and analyses the known or foreseeable risks associated with each system;

(b) estimate and assess the risks that may arise when the system is used as intended or under inappropriate but reasonably foreseeable conditions of use;

(c) examine other risks that may arise, based on data collected from post-market monitoring;

(d) adopt appropriate risk management measures.

These latter measures must be implemented taking into account the possible effects and interactions that may result from the combined application of all the requirements provided by the relevant legislation and the current state of technology, generally recognized. The measures will aim to eliminate, reduce, or mitigate risks. To identify the most appropriate risk management provisions, high-risk AI systems will be tested at any time during the development process, prior to introducing the system to the market or before putting it into operation.

Regarding data governance, high-risk AI systems involving training data models will be developed based on training, validation, and testing datasets that must be relevant, representative, complete, and error-free. The regulation provides for the possibility for providers of these systems to process special categories of personal data, to the extent that

this action is strictly necessary to ensure monitoring, detection, and correction of systematic errors, subject to proportional guarantees for the fundamental rights of individuals (EDPB-EDPS, 2021; EDPS, 2023).

The requirement regarding the technical documentation of a high-risk system entails its preparation prior to the introduction of the system to the market and the obligation to update it. The documentation aims to demonstrate the system's compliance with all requirements and to provide competent national authorities with all necessary information to evaluate the system's conformity with the Regulation.

The obligation of transparency involves designing and developing a high-risk AI system in a sufficiently clear manner to allow users to interpret the system's results and use it properly. The level of transparency provided must be adequate to enable both the user and the provider to fulfil their obligations under the Regulation. Transparency can be manifested in a user manual for the system's use, in digital format, or in other ways by providing concise, complete, and coherent information in an accessible and predictable manner for users. The informational tool will contain details regarding the identity and contact information of the provider, the characteristics, capabilities, and limitations of the system's performance (its purpose, level of accuracy, and cybersecurity, the individuals with whom the system is intended to be used), and, where applicable, changes made to the system, the expected lifespan, and any maintenance measures necessary for the proper functioning of the system (including software updates). Considering the specific risks of manipulation posed by AI systems, Article 52 of the AI Act establishes transparency obligations for systems that: "(i) interact with humans, (ii) are used to detect emotions or determine association with (social) categories based on biometric data, or (iii) generate or manipulate content (“deepfakes”)" (Point 5.2.4 in the Explanatory Memorandum of the AI Act Proposal).

After the high-risk systems are placed on the market, their use must be effectively monitored by individuals to prevent or reduce existing risks to fundamental rights that may arise from the use of the systems. Those responsible for monitoring must fully understand the capabilities and limitations of a system so that they can properly monitor its operation and promptly report any anomalies, malfunctions, or unexpected performances. Additionally, supervisors must be able to correctly interpret the results of the high-risk AI system and decide, in any particular case, not to use the system. Finally, measures to ensure human oversight must allow individuals to intervene in the operation of the high-risk system, including being able to interrupt the system through a "stop" command or similar procedure.

Banned or Prohibited AI systems. Certain uses of AI present such a high risk that it is considered unacceptable and the use of such a system in the EU should be prohibited. The category of unacceptable risks should be understood as any artificial intelligence system whose use would undermine the values of the Union, for example by violating fundamental rights. The first mention of prohibited practices appears in the preamble of the Regulation and explains at length the background and reasons for the existence of this category - "aside from the many beneficial uses of artificial intelligence, that technology can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and should be prohibited […]" (recital 15 AI Act). Broadly speaking, the list of prohibited practices under the AI Act covers four distinct types of AI (Uscov S., Groza A., 2022). The first relates to subliminal AI practices,

i.e. those with significant potential for cognitive-behavioural manipulation of individuals. The second set are methods that exploit the weaknesses of specific vulnerable groups ("exploitative AI practices"), such as children and people with disabilities. For both sets to fall into the category of unacceptable risk systems, they must be used to distort a person's behaviour in a way that causes or is likely to cause physical or psychological harm to that person. The third set comprises social scoring systems, i.e. programmes used by public authorities or other agents, but on behalf of the state, to assess or classify the reliability of citizens over a period of time according to their social behaviour and personality traits. Finally, the fourth category consists of real-time remote biometric identification systems, which involve the use of AI in public places for law enforcement purposes. Thus, this type of AI is not allowed to extract sensitive data (sexual orientation, religious denomination) or in law enforcement based on predictive person analysis.

The AI Act also prohibits the use of facial images from the internet or video monitoring systems (such as CCTV footage) for unspecified and non-explicit collection purposes, as well as the recognition of emotions in the workplace or in educational institutions.

Each prohibited practice raises serious regulatory challenges, made more difficult by the inherent interconnectedness of systems caused by the general trend towards convergence of existing products, industries and technologies. Experts argue that the overall balance and integrity of the legal system is challenged precisely by the inherent interdependence of AI systems, which creates the need for sufficiently specific and comprehensive regulation capable of being applied to as many distinct factual situations as possible (Neuwirth R.J., 2023).

3. Penalties according to AI Act

Regarding the sanctioning system, the Regulation establishes the maximum limits of fines for specific violations, leaving it to the discretion of the Member States to establish rules regarding sanctions, including administrative fines applicable in case of non-compliance with this Act. Broadly speaking, the sanctions provided by the Regulation target three categories of subjects: operators of AI systems, providers of general-purpose AI systems, and Union institutions, bodies, and agencies. Depending on the maximum amount of the fine that can be imposed, the sanctions are grouped into three levels. The first level refers to violations of the prohibitions imposed by Article 5 AI Act ("Prohibited Practices in the field of AI"), the second encompasses non-compliance with the obligations provided by the Regulation, and the last level involves the incorrect provision of information to authorities.

a) Non-compliance with the prohibitions imposed by the Regulation

The highest fines are applied for the use or placing on the market of systems prohibited by the Regulation due to the unacceptable level of risk they pose. These situations are subject to fines of up to €35,000,000 or, in the case of a company, up to 7% of its total annual worldwide turnover for the preceding financial year. This amount exceeds the penalties provided by the GDPR (4%) or the Digital Services Act (6%), imposing some of the most severe non-compliance sanctions in the EU. Penalties will be applied for the use in the Union of any of the systems listed in Title II of the Regulation, such as systems that implement manipulation techniques with distorting effects on individuals' behaviours or those that classify individuals based on their biometric data to infer their race, political opinion, religious belief, sexual orientation, etc.

b) Non-compliance with the obligations imposed by the Regulation
The second-largest category of fines is established for the failure to comply with specific obligations by different subjects and has a maximum amount of €15,000,000 or up to 3% of the annual global turnover for enterprises. These sanctions will be applicable in case of failure to comply with: a) the obligations of providers of high-risk AI systems (provided for in Article 16 of the Regulation); b) obligations of authorized representatives; c) obligations of importers and distributors; d) obligations of deployers;
According to Article 25 of the Regulation, an authorized representative is any natural or legal person established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to carry out and fulfil, on behalf of the provider, the obligations and procedures established by this regulation. Thus, representatives must act in accordance with the mandate received from the provider and in accordance with the obligations established by the aforementioned article. An importer is considered to be any natural or legal person established in the Union who places on the market an AI system bearing the name or trade name or the mark of a natural or legal person established outside the EU. Importers are obliged to ensure that the high-risk AI systems they place on the market comply with this regulation. Similarly to importers, distributors must ensure the conformity of the system with the relevant legislation and cooperate with the competent authorities.
According to art. 3 AI Act, a deployer (or user) represents an entity that uses an AI system under its authority, and this use is carried out as part of a professional activity. Users of high-risk systems are primarily obliged to use the systems in accordance with the provided instructions and to take appropriate measures to supervise the systems.
c) The supply of incorrect, incomplete or misleading information to authorities
Failure to provide correct and complete information constitutes a violation of Article 23 of the Regulation, which requires cooperation between providers and competent authorities. Thus, providers of high-risk AI systems are obligated to provide national authorities, upon request, with all the necessary information and documentation to demonstrate the system's compliance with the requirements established by law. If the information provided is incorrect, incomplete, or misleading, providers may face fines of up to €7,500,000 or up to 1% of the total worldwide turnover for companies. In applying sanctions, competent authorities will consider that the measures taken should be effective, deterrent, and proportionate to the type of action, the party's previous conduct, and its profile. Factors that may be taken into account in individualizing sanctions include: a. the nature, gravity, and duration of the offense; b. the intentional or negligent nature of the violations; c. measures taken to mitigate the effects of the violation; d. the harm caused or gains made through the violation. In any case, the AI Act recognizes the diversity of practical cases, therefore it regulates only the maximum threshold of fines and provides special provisions for smaller or newly established enterprises.

Conclusions

Artificial Intelligence is a disruptive technology that can be used as an accelerator for innovation in all scientific fields, as well as in industry or the business environment. The synergy between AI and new technologies such as Machine Learning and Cloud computing can rapidly and efficiently propel technological advancement and improve people's quality of life. Harnessing the opportunities offered by AI generates significant risks to

fundamental rights and values, which justifies regulating how AI systems are developed, implemented, and used by directly assessing their potential risk level. The emergence of the AI Act and the establishment of the European AI Office are, in our view, just the beginning of regulating how AI is developed and used. The complexity of AI systems and the diversity of fields in which it is used necessitate much stricter rules for certifying an AI system as safe and trustworthy than those proposed at the EU level through the AI Act. We believe that the efforts made at the EU level represent only the first steps towards a comprehensive legal mechanism that would require EU AI Office verification and approval of any AI system before it is introduced to the European digital market.

References

1. Ad Hoc Committee on Artificial Intelligence (CAHAI) AI Ethics Guidelines: European and Global Perspectives, June 15th, 2020. Retrieved from https://rm.coe.int/cahai-2020-07-fin-en-report-ienca-vayena/16809eccac.
2. Ad Hoc Committee on Artificial Intelligence (CAHAI), Feasibility Study, December 17th, 2020. Retrieved from: https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da;
3. Alzoubi, A.A., Al Aqeel, I., Alzoubi, H.M. (2024). Review of Artificial Intelligence and Machine Learning Recent Advancements. Alzoubi, H.M., Alshurideh, M.T., Vasudevan, S. (eds) Technology Innovation for Business Intelligence and Analytics (TIBIA). Studies in Big Data, vol 147. Springer, Cham. Retrieved from: https://doi.org/10.1007/978-3-031-55221-2_14.
4. Anyoha R. (2017) The History of Artificial Intelligence. Harvard Science In The News, August 28th, 2017, Retrieved from: https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/.
5. Brue M. (2023) Microsoft Introduces Generative AI Tools To Boost Creativity, in Forbes.com website. Retrieved from: https://www.forbes.com/sites/moorinsights/2023/10/10/microsoft-introduces-generative-ai-tools-to-boost-creativity/?sh=56fb2d1c5469
6. Committee On Artificial Intelligence (CAI) Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule Of Law, December 18th, 2023. Retrieved from: https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043.
7. Council of Europe, Towards Regulation of AI Systems. Global perspectives on the development of a legal framework on Artificial Intelligence (AI) systems based on the Council of Europe's standards on human rights, democracy and the rule of law, December 2020. Retrieved from: https://rm.coe.int/prems-107320-gbr-2018-compli-cahai-couv-texte-a4-bat-web/1680a0c17a.
8. EDPB-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act). Retrieved from: https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf;
9. EDPS, Opinion 44/2023 on the Proposal for Artificial Intelligence Act in the light of legislative developments. Retrieved from: https://www.edps.europa.eu/system/files/2023-10/2023-0137_d3269_opinion_en.pdf.
10. European Commission, White Paper on Artificial Intelligence - A European approach to excellence and trust, Brussels, 19.02.2020, COM (2020) 65 final. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0065.
11. Halford C., Air C., Eastwood H., (2022) EU Data Package. Lexology Website. Retrieved from: https://www.lexology.com/library/detail.aspx?g=e73ff151-08a2-41dc-b845-d2484b5fb5be
12. High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, April 8th, 2019. Retrieved from: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.
13. Hintze A. (2016). Understanding the four types of AI, from reactive robots to self-aware beings, November 14th, 2016. Retrieved from: https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-6761
14. Laux J., Wachter S., Mittelstadt B. (2024). Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. Regulation & Governance, 18: 3-32. Retrieved from: https://doi.org/10.1111/rego.12512.

15. Moor J. (2006). "The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years", AI Magazine, 27(4), p. 87. doi: 10.1609/aimag.v27i4.1911.
16. Neuwirth R.J. (2023) Prohibited artificial intelligence practices in the proposed EU Artificial Intelligence Act (AIA). Computer Law & Security Review, Volume 48, 2023, DOI: https://doi.org/10.1016/j.clsr.2023.105798. Retrieved from: https://www.sciencedirect.com/science/article/pii/S0267364923000092.
17. OECD Principles for Artificial Intelligence, Retrieved from: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#adherents.
18. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496.
19. Proposal for a Regulation of The European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), as approved by the European Parliament on March 13, 2024. Retrieved from: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf
20. Tabsharani F. (2023). Types of AI algorithms and how they work, May 5th, 2023. Retrieved from: https://www.techtarget.com/searchenterpriseai/tip/Types-of-AI-algorithms-and-how-they-work
21. Ungureanu C.T. (2021) Drept internațional privat european în raporturi de comerț internațional, Ed. Hamangiu, București, 2021.
22. Ungureanu C.T., Amironesei A.E. (2023) Legal issues concerning Generative AI technologies. Eastern Journal of European Studies, Volume 14, Issue 2, December 2023, DOI: 10.47743/ejes-2023-0203. Retrieved from: https://ejes.uaic.ro/articles/EJES2023_1402_UNG.pdf.
23. Uscov S., Groza A. (2022) Cât de inteligent este Artificial Intelligence Act?. Curierul Judiciar nr. 2/2022.