RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
March 12-13, 2026
DOI:10.5281/zenodo.19553532

AI and the World We Live In

Raluca-Mihaela Nanu

Law office of „Nanu Raluca-Mihaela", Bucharest Bar Association, Bucharest, Romania
av.ralucananu@gmail.com

Abstract: In the world we live in, we are no longer alone. We have created a force that is next to us, step by step. We created it to help us. The question is how far we let it run „free" and to what extent we can use it. States have begun enacting laws regulating the use of AI to ensure fundamental human rights are respected. A set of prohibited practices is being developed worldwide, aimed not at limiting technological development but at protecting individuals. Most countries have adopted a risk-based approach. There is, however, a fundamental difference between these normative acts: technologically developed states have adopted measures more "gentle" for the use of AI, prioritizing speed over caution that might be excessive in certain legislations. This article proposes a brief analysis across different regulations, starting from the European AI Act and continuing with a general presentation of non-European rules on the use of AI.

Keywords: AI, Prohibited Practices, High-Risk Systems, General-Purpose Systems, Biometric Identification

Introduction

In the last few years, AI has been widely used in almost all areas of activity. Biometric identification systems have been created through which people can be monitored or with the help of which they can carry out various daily activities. For example, simply accessing your own phone can be done through facial identification. Furthermore, an increasing number of devices are equipped with AI systems that are able to perform tasks extremely quickly, which would take people much longer to accomplish. AI is constantly trained with data, becoming increasingly more efficient. In light of these developments, states have begun to develop standards for the use of AI in order to protect fundamental human rights, emphasizing that technological progress is made for humanity and not against it, thereby placing the human being at the center of technological evolution.

1. The Legal Framework of AI in Europe

1.1. The history of the AI Act

At the European level, it has been decided that AI use has reached a point where certain limitations should be imposed. Thus, the European Commission (2020) report on the safety and liability implications of artificial intelligence, the internet of objects and robotics states that "Unintended effects originating from AI could cause harm to users and exposed individuals."

In a similar vein, the European Parliament (2020) Resolution of October the 20, 2020, with recommendations to the Commission on the framework for ethical issues associated with artificial intelligence, robotics and related technologies (2020/2012(INL) emphasizes that AI is human-centered and man-made, considering that "there is a need for an effective and harmonized regulatory framework based on Union law, the Charter and international human rights law, to be applied in particular to high-risk technology, in order to establish equal standards across the Union and effectively protect Union's values". In the same vein, the European Parliament "underlines the asymmetry between those who use AI technology and those who interact with it; underlines, in this context, that citizens' trust in AI can only be achieved if a „rulebook of default ethics is ensured and from the time of design", which guarantees that any given AI in use fully complies with the Treaties Charter of fundamental rights and secondary law of the Union". The following year, member states improved the Coordinated Plan for AI by aiming to transform AI into action by accelerating investment in

AI technology by adopting new digital solutions and maximizing their advantages through the implementation of AI strategies and programs (European Commission, 2021).

Finally, the AI Act was adopted by the Council on May 21, 2024, and on June 13, 2024, EU Regulation 2024/1689 of the European Parliament and of the Council was adopted. It is worth mentioning a particular passage of the speech of the Belgian State Secretary for Digitization, in charge of administrative simplification, privacy protection and the state property management agency delivered before the Council in May 2024: "The adoption of the IA Act is an important step for the European Union. This legislative act, the first of its kind in the world, addresses a global technological challenge that also creates opportunities for our societies and economies. With the IA Act, Europe underlines the importance of trust, transparency and accountability in new technologies, while ensuring that this fast-moving technology can thrive and drive European innovation" (Nanu, 2025, p. 17; Council of the European Union, 2024).

1.2. AI Risk Levels

The AI Act is the cornerstone of legal provisions regarding the limitations on the use of AI systems, being the first legal act that uses a risk classification to establish these limitations.

a) It must be said that the majority of AI applications currently available on the EU single market, such as AI-enabled video games and spam filters, have a **minimal risk**. It is important to note that these types of systems are unregulated.

b) Under the AI Act, **general-purpose AI models** are classified within the lowest-risk category. The Act defines them as "an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications" (Article 3(63) AI Act).

According to recital 98 AI Act, "whereas the generality of a model could, inter alia, also be determined by a number of parameters, models with at least a billion parameters and trained with a large amount of data using self-supervision at scale should be considered to display significant generality and to competently perform a wide range of distinctive tasks." This recital must be corroborated with the next recital of AI Act that adds the following: "large generative AI models are a typical example for a general-purpose AI model, given that they allow for flexible generation of content, such as in the form of text, audio, images or video, that can readily accommodate a wide range of distinctive tasks."

Taking into consideration the evolving state-of-the-art, it must be said that general-purpose AI models with systemic risk may change over time. But what are systemic risks? A very good explanation is given by the European Commission according to which: "They are risks of large-scale harm from the most advanced (i.e., state-of-the-art) models at any given point in time, or from other models that have an equivalent impact (see Article 3(65) AI Act). Such risks can manifest themselves, for example, through the lowering of barriers for chemical or biological weapons development, or through unintended issues of control over autonomous general-purpose AI models (recital 110 AI Act). The most advanced models at any given point in time may pose systemic risks, including novel risks, as they are pushing the state of the art. At the same time, some models below the threshold corresponding to the state of the art may also pose systemic risks, for example, through reach, scalability, or scaffolding." (European Commission, 2025)

There are two dates of entry into force for AI Act provisions regarding these types of models: August 2, 2025, for general-purpose AI models placed on the market on or after that date, and August 2, 2027, for general-purpose AI models placed on the market before August 2, 2025.

c) Another category of systems subject to the AI Act is that of **high-risk systems** that must meet strict requirements and obligations in order to be used on the EU market (rigorous testing, human supervision, transparency). These systems are subject to the provisions of Article 6 of the AI Act, according to which two conditions must be met cumulatively in order for an AI system to be considered a high-risk:

"- is intended to be used as a safety component of a product or is itself a product subject to the Union harmonization legislation set out in Annex I;

- the product for which the AI system or the AI system itself is intended, if it is itself produced on its own, is subject to a conformity assessment by a third party with a view to being placed on the market or to be put into service." (Article 6 (1) AI Act)

High-risk AI systems are listed in Annexes I and III of the AI Act.

Annex I includes AI systems that are subject to the regulations of several European Directives, being thus brought together at the legislative level in the category of high-risk systems. This category includes, for example: technical equipment (safety components; lifting accessories; chains, cables and webbing, etc.), playground equipment for public use; automated entertainment machines, pleasure boats and watercraft, boats undergoing major transformation, as well as the following components if produced outside the EU: flame-retardant equipment for inboard engines and inboard motors with steerable propellant operating on petrol and for spaces intended for petrol tanks, safety components for lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, new cable installations intended for the transport of persons, appliances consuming gaseous fuels, medical devices for human use and accessories for such devices.

Also, the high-risk systems are part of the systems included in Annex III of the AI Act, such as those used biometric identification of persons involved in investigations or criminal activities, systems that are used in critical infrastructure, those used in the field of education and professional training, in the field of employment, worker management and access to independent activities AI systems on access to essential private services and public services and benefits, AI systems used in law enforcement, in the areas of migration, asylum and border control management, AI systems used in the administration of justice and democratic processes.

There are two dates for the entry into force of the AI Act provisions regarding these types of models: August 2, 2026, for designated high-risk AI systems (Annex III) placed on the market after that date, or those placed on the market before August 2, 2026, that are subject to significant change in their design; and August 2, 2027, for regulated product and safety component high-risk AI systems (Annex I) placed on the market after August 2, 2026, or those placed on the market before that date that are subject to significant change in their design.

d) The most dangerous AI systems are those classified as **unacceptable risk**, which are subject to prohibited practices at the European level, being extensively debated in Article 5 of the AI Act. Thus, it is forbidden to use AI systems in the European Union that pose a threat to the safety, rights or livelihoods of people such as: behavioral-cognitive manipulation, police activities based on predictive analysis, recognition of emotions at work and educational institutions, attribution of a social score, making assessments or classifications of people according to social behavior or personal or personality characteristics known or deduced or predicted based on algorithms, learning institutions detecting the criminal potential of a person using solely the profile of that person or assessing his or her personality traits and characteristics. At the same time, it is forbidden to create or expand facial recognition databases by extracting facial images from the Internet or CCTV recordings without a precise purpose, as well as the use of biometric identification systems at a distance in real time (facial recognition in public spaces by law enforcement authorities), these two categories of

prohibitions having certain discussions. Thus, extracting a person's facial record can be done if the purpose for which it is done requires it; for example, for the discovery of a person involved in either a crime or another easier violation of the law (a contravention). This results from the interpretation of the phrase "without specific purpose" found in the text of Article 5 (e). Regarding biometric identification, besides the facial identification that is most often used, other biometric features used to identify a person are: digital fingerprint, voice fingerprint, iris, retina, hand geometry, handwriting, finger shape. Being the most used biometric identification method and also involving the processing of personal data, it was considered necessary to adopt at European level, before the AI Act, the Guidelines no. 5/2022 on the use of this technology, document in which are given examples of facial recognition: "searching, in a photo database, the identity of an unidentified person (victim, suspect, etc.), monitoring the movements of a person in the public space, reconstructing the journey of a person and subsequent interactions with other people, remote biometric identification in public spaces of the people sought, automatic recognition of people in an image to identify, for example their relationships on a social network that uses this type of recognition, access to services, some cash dispensers recognizing their customers, by comparing a facial capture made by a camera with the database of facial images held by the bank, tracking the journey of a passenger at a certain stage of the journey" (paragraph 22).

However, real-time remote biometric identification can be of real use when used for law enforcement and the defense of people who are victims of a crime. In this respect, the AI Act points out in Article 5 (h), (i), (ii), (iii), which are the exceptions allowing remote biometric identification in real time, and Annex II specifies the offences for which such systems are assigned to a person:

"- whether the purpose of this action is either to search for a missing person or to identify the victim of a kidnapping or trafficking in human beings or sexual exploitation;

- whether real-time biometric identification is aimed at preventing the consequences of a threat to a person's life or safety or preventing a terrorist attack;

- whether real-time biometric identification is aimed at identifying or locating a person prosecuted for the commission of a crime or prosecuted for the execution of a custodial sentence or a custodial security measure for a maximum period of at least 4 years."

"The offences for which the use of AI systems for real-time biometric identification is permitted are those set out in Annex II of the IA Act, namely: terrorism; trafficking in human beings; sexual exploitation of children and child pornography; illicit trafficking in narcotic drugs or psychotropic substances; illicit trafficking in arms, munitions or explosive substances; murder, serious bodily harm; illicit trafficking of human organs or tissues; illicit trafficking of nuclear or radioactive materials; abduction, unlawful deprivation of liberty or hostage-taking; offences within the jurisdiction of the International Criminal Court; unlawful seizure of aircraft or ships; rape; environmental crimes; organized or armed robbery; sabotage; participation in a criminal organization involved in one or more of the offences listed above" (Nanu, 2025, p. 82).

It is worth mentioning that biometric identification can also be used in cases where it does not conflict with the provisions of Article (9) of the General Regulation on data protection (Regulation (EU) 2016/679), even if it is not about law enforcement or helping people who are victims of a crime. For example, if the person has given his explicit consent to the processing of this personal data, if the processing is necessary to protect the vital interests of the person, when the processing is necessary for reasons of major public interest, biometric identification may be used. Legal provisions regarding these types of AI systems entered into force on February 2, 2025.

2. The Legal Framework of AI in Non-European Countries

United States of America

In 2025, the US National Strategy on AI was adopted to pursue "the centralization of artificial intelligence regulation at the federal level, with the objective of preventing the 50 federal states from achieving it at their level and thus to have a single source of authorization. The text aims to ensure an artificial intelligence that operates in a single legal framework" (Duțu, 2025). Unlike regulation in Europe, the US is focusing on innovation, promoting less restrictive regulation, focusing on the use of AI as a tool for economic growth and strategic positioning.

In March 2026, the U. S. adopted a seven-pillar set of regulations for artificial intelligence to be subject to the adoption of Congress. The seven pillars are child protection, protection and consolidation of American communities, intellectual property and protection of creators, the prevention of censorship and the protection of freedom of expression, American innovation and dominance in AI, education and workforce prepared for AI, a unitary federal framework and the pre-emption of state laws.

The seven-pillar proposals show that the US is moving forward with the idea of developing artificial intelligence rapidly, being much less restrictive of European regulation, but at the same time protecting American citizens from the dangers of reckless use of AI.

It follows that the Congress, to debate this set of regulations, after the adoption of – in the current or modified form – will have the power of law.

South Korea

The first country in the world to adopt a comprehensive legislative framework on the use of AI is South Korea, which legislated a legislative package on 22 January 2026 to regulate AI. South Korea's regulation introduces „the obligation of human surveillance for high-impact artificial intelligence applications, which include areas such as nuclear safety, drinking water supply, transport, health and financial services", as well as the obligation for companies to inform „users in advance when their products or services use artificial intelligence and clearly mark the content generated by AI" (Mocanu, 2026).

Unlike all other regulations for AI that are limited to a single law, South Korean regulation contains a legislative package that contains measures that relate to both regulating and promoting the development of AI. In addition to setting safety standards, it was also aimed at promoting innovation and strengthening South Korea's position in the technology industry.

China

Before 2023, biometric identification systems were used in China, mainly facial identification without the consent of citizens, being classified based on social scores obtained from the analysis of people's behavior. For example, in order to get a bank loan, the person had to have a certain score. The same was the case for someone to be able to make a reservation in a particular hotel or restaurant. To achieve facial identification, there was a camera that was absolutely everywhere: at work, in hotels, restaurants, places to relax, on every street, in every intersection. Any violation of the rules was penalized by lowering the social score. The citizens had a specific application installed on their phone that they were notified when their social score changed, in addition, or minus. In 2019, China introduced mandatory facial recognition for mobile phone users, used whenever they want to register on the platforms of new mobile services (Petcu, 2019).

Things began to change since 2023 when China developed new rules on the use of facial recognition technology. These rules were intended to restrict the use of this technology by companies in favor of non-biometric personally identifiable methods that require the

individual consent of each person and require a specific purpose for the use of facial recognition. However, in case of administrative situations (unspecified), the agreement is not required. According to the project, biometric identification systems related to facial identification in public spaces can be used only to maintain public safety, and their existence in areas such as hotels, airports, train stations, exhibitions, stadiums, and banks should be prohibited, except for certain legal provisions that are not specified in the project. Also, according to the same law, even if facial identification systems are prohibited in intimate spaces, however, such systems can be used without restrictions when they are used for AI training. If motivated in this way, the use of facial identification systems no longer requires any consent from citizens, they are simply obliged to accept them wherever they are placed.

On 15 August 2023, the regulation on artificial intelligence generative entered into force, the purpose of which is to „promote the healthy development and standardized application of generative artificial intelligence, protect national security and public interests, and protect the legitimate rights and interests of citizens, legal persons and other organizations" (Article (1)).

According to Article (2) "This Regulation does not apply to industrial organizations, enterprises, educational and research institutions, public cultural institutions and relevant professional institutions that develop and apply generative artificial intelligence technology but do not provide generative artificial intelligence services to the public in China." It is specified in the Regulation that "in the process of designing algorithms, selecting training data, generating and optimizing models and providing services, effective measures will be taken to prevent discrimination on the grounds of ethnicity, beliefs, nationality, region, gender, age, occupation, health, etc" (Article (4)(ii).

In 2025, China launched digital identity cards that allow users to log in before they can use the internet. Chinese students can also use, in addition to these bulletins, a facial recognition system that allows them access to schools and pay for their lunch (Sabău, 2025). According to the same source, "Police uses – for seven years already – glasses equipped with facial recognition technology to spot suspects."

Vietnam

On 10 December 2025, Law No. 134/2025/QH15 on Artificial Intelligence (the "AI Law") was adopted by the National Assembly of Vietnam. Vietnam thus becomes the first Southeast Asian state to adopt a comprehensive regulatory framework targeting AI. The law is based on the four-level risk classification system, similar to the European AI Act. Like European law, Vietnamese law applies to both Vietnamese and foreign producers, distributors and users, and the rules containing specific sanctions for non-compliance will be published as soon as possible.

Brazil

In Brazil, the Chamber of Deputies is expected to adopt the legislative regulation of artificial intelligence - Brazil AI Act – probably during this year, given the fact that on December 10, 2024, the Brazilian Senate approved Bill No. 2338/2023, which sets out rules for developing and using artificial intelligence in Brazil. According to the Artificial Intelligence Act website (2024), "The Bill takes a risk-based approach to regulating AI systems. It places stricter rules on high-risk systems, especially those that could affect public safety or fundamental human rights. It also requires AI developers and users to make their systems fair, transparent, and easy to understand. The Bill aligns with Brazil's General Data Protection Law (LGPD) to protect privacy. Additionally, it plans to create a new authority to oversee AI regulations and enforce the rules." According to the same source, "The penalties for non-compliance with the Bill can go up to BRL 50 million (approx. $1.6 million) or 2% of the total turnover of the company."

Conclusion

An increasing number of countries have begun legislating the use of artificial intelligence following Europe's adoption of regulatory measure in 2024. It can be observed that there are different approaches, and that highly developed countries approach the use of AI less responsive to others. There must be a balance between the safety of using AI and the development of new technologies. While regulation is necessary, overly strict regulation could slow innovation, which is not desirable, but the fundamental rights of citizens must be respected.

References

Artificial Intelligence Act website. (2024*). Brazil AI Act*. https://artificialintelligenceact.com/brazil-ai-act/

Council of the European Union. (2024, May 21). *Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI* (Press release). https://www.consilium.europa.eu/ro/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/

Council of the European Union. (n.d.). *Artificial intelligence policy.* https://www.consilium.europa.eu/ro/policies/artificial-intelligence

Duțu, M. (2025). *Artificial intelligence law in the current U.S. strategy.* https://www.juridice.ro/

European Commission. (2020). *Report on the safety and liability implications of artificial intelligence, the internet of things and robotics.* https://commission.europa.eu/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en

European Commission. (2021, April 21). *Coordinated plan on artificial intelligence: 2021 review*. https://digital-strategy.ec.europa.eu/en/policies/plan-ai

European Commission. (2025, September 9). *General-purpose AI models in the AI Act: Questions & answers*. https://digital-strategy.ec.europa.eu/en/faqs/general-purpose-ai-models-ai-act-questions-answers

European Parliament (2020). *European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies* (2020/2012(INL)). https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52020IP0275

Mocanu, R. (2026). *South Korea adopts the world's first comprehensive laws for regulating artificial intelligence.* Mediafax, January 22. https://www.mediafax.ro/stirile-zilei/coreea-de-sud-adopta-primele-legi-cuprinzatoare-din-lume-pentru-reglementarea-inteligentei-artificiale-23674771

Nanu, R. (2025). *Regulamentul privind inteligență artificială – comentariu pe articole*, 17, 82 [The regulation on artificial intelligence]. Universul Juridic Publishing House.

Petcu, A. (2019). *China introduces mandatory facial recognition for mobile phone users.* Mediafax, December 1. https://www.mediafax.ro/life-inedit/china-introduce-recunoasterea-faciala-obligatorie-pentru-utilizatorii-de-telefoane-mobile-18637109

Porojan, T. (2026). *The United States has published the legislative framework for artificial intelligence. Financial Market.* https://financialmarket.ro/fintech/artificial-intelligence/statele-unite-au-publicat-cadrul-legislativ-pentru-inteligenta-artificiala-7-piloni-care-vor-remodela-industria-tech-globala/

Sabău, A. (2025). *China is using new technologies at full speed*. Gandul, October 11. https://www.gandul.ro/international/china-recunoasterea-faciala-folosita-pentru-a-permite-accesul-elevilor-in-scoli-dar-si-pentru-a-repera-fugarii-de-lege-in-multime-20664672