www.amcham.hr

Američka gospodarska komora u Hrvatskoj | American Chamber of Commerce in Croatia

Zagreb, July 2026

Criminal Liability Framework in the Use of Artificial Intelligence

Table of Contents

Introduction

Artificial intelligence (AI) is becoming a key technology for enhancing productivity, competitiveness and the innovation capacity of the economy. Its application is already transforming business processes, driving the development of new products and services, and creating opportunities for economic growth.

At the same time, the development and deployment of AI systems raise new questions relating to safety, liability and risk management, particularly where the use of such systems may result in harm to individuals, organizations or society as a whole.

In October 2025, amendments to the Croatian Criminal Code introduced a new criminal offense: "Causing Danger Through the Use of an Artificial Intelligence System" (Article 215a).

> *"Whoever, in the development, testing, verification, supervision, management or use of an artificial intelligence system, or otherwise through an artificial intelligence system, causes danger to the life or physical integrity of persons or to property of substantial value, provided that a more serious criminal offense has not thereby been committed, shall be punished by imprisonment for a term or six months to five years."*

This is the first provision in Croatian legislation to expressly address the potential risks arising from the development, testing, supervision, management or use of AI systems. The Criminal Code also provides for more severe penalties where such conduct results in serious bodily injury, significant property damage, or the death of one or more persons. While the primary objective of this provision is to protect life, health, and property from risks associated with potentially hazardous technological systems, its wording raises several important legal issues concerning the scope of criminal liability, the requirement of legal certainty, its relationship with existing criminal offenses, and its alignment with the European regulatory approach.

AmCham supports the establishment of a regulatory framework that ensures a high level of protection for individuals and society against harmful consequences. However, we believe that the current framework creates regulatory uncertainty for the business community developing or using AI systems, which may adversely affect investment, innovation, and the broader adoption of new technologies in Croatia.

The purpose of this paper is to identify the key challenges arising from the current framework and propose amendments that would better balance public protection with an environment conducive to innovation and the deployment of new technologies.

Shortcomings of the Current Framework

Overly Broad Definition of Potentially Liable Persons

One of the key challenges posed by Article 215a is the very broad range of persons who may be subject to criminal liability. The provision covers the development, testing, verification, supervision, management and use of AI systems, thereby potentially encompassing virtually every participant in an AI system's lifecycle:

- AI system programmers and developers;
- individuals responsible for testing or validating models;
- businesses implementing or integrating AI systems into their operations;
- system operators and administrators;
- end users.

This approach reflects the fact that AI is the product of complex technological and organizational processes involving multiple actors. However, the Criminal Code does not specify which particular acts performed at the various stages of development or deployment give rise to criminal liability, creating uncertainty as to the point at which criminal liability arises.

For the business community, it is essential that the regulatory framework be clear and predictable. Where the boundaries of liability are not sufficiently well defined, legal uncertainty increases, making investment and business decision-making more difficult. If a legal provision is drafted too broadly or too vaguely, there is a risk that its practical scope will ultimately be defined through case law. While courts routinely develop the interpretation of general legal concepts, criminal law seeks to avoid situations in which the limits of criminal liability are left to the broad discretion of courts or prosecutorial authorities.

An additional challenge arises from the very nature of AI systems. A harmful event may result from a combination of factors, including algorithm design, the quality of training data, the manner in which the system is implemented, or the way it is used. In such circumstances, it may be difficult to determine precisely whose specific conduct gave rise to the danger or harm.

In light of the above, it is questionable whether the provision fully satisfies the requirements of clarity, precision and foreseeability that are fundamental to criminal law. In our view, criminal liability relating to AI should be linked to specific breaches of regulatory obligations, safety standards or requirements established under the European regulatory framework governing AI. Such an approach would provide greater legal certainty for the business community and encourage innovation, while maintaining effective protection against genuinely dangerous conduct.

The Vague Definition of "Causing Danger"

Criminal law requires both prohibited conduct and its consequences to be clearly defined in order to ensure legal certainty and the foreseeability of criminal liability. However, the AI criminal liability provision establishes criminal liability already for "causing danger" to life, physical integrity or property of substantial value.

Such an approach may prove difficult to apply in practice for several reasons:

- it is not always clear when a particular technological error constitutes a genuine danger; and
- the line between a technical defect and criminally relevant danger may be unclear.

A further challenge lies in the fact that the concept of danger is open to different interpretations. It may refer either to a concrete and imminent danger or to an abstract possibility of harm. As the legislation does not specify which type of danger is intended, there is a risk that the boundary between lawful and criminal conduct will remain uncertain. This is particularly significant in the context of AI, where certain risks are inherent in the development, testing and deployment of new technologies.

In practice, much will therefore depend on how courts interpret the concept of danger and under what circumstances they consider the threshold for criminal liability to have been met. This, in turn, undermines legal certainty and predictability.

Relationship with Existing Criminal Offenses

Many situations that may arise from the use of AI are already covered by existing criminal offenses.

For example, the Criminal Code already contains provisions relating to:

- Endangerment to Life and Property by a Generally Dangerous Act or Means (Article 215 of the Criminal Code),
- Property Damage (Article 235 of the Criminal Code),
- Destruction of or Damage to Safety Devices at Work (Article 217 of the Criminal Code).

In this context, the introduction of a separate AI-related criminal offense may be viewed as a symbolic provision intended to emphasize the specific risks associated with emerging technologies. AI may be regarded as one of the technical means through which harmful conduct is carried out, in much the same way that criminal law already addresses offenses committed using machinery, vehicles or information systems.

Even if this criminal provision is rarely applied in practice, its impact may nevertheless be significant because it increases the perceived regulatory risk for the business community. This perception can have a substantial effect on the investment climate and business planning.

Businesses developing or deploying AI systems face uncertainty as to:

- what specific conduct may give rise to criminal liability;
- who within an organization may be held liable, such as a developer, manager or system operator; and
- how courts will interpret concepts such as "danger" and "negligence" in the context of AI.

This uncertainty may prompt businesses to adopt a more cautious approach to the development and deployment of new technologies in order to mitigate regulatory risk. Further uncertainty arises from the combination of a relatively broad basis for criminal liability and very severe penalties, including lengthy terms of imprisonment in cases involving the most serious consequences. Consequently, this may lead to reduced investment in emerging technologies, underutilization of AI's potential in the Croatian economy, a more cautious approach to introducing innovations, and the redirection of investment toward markets with more innovation-friendly regulatory environments. This particularly affects startups, small and medium-sized enterprises (SMEs), and research organizations, which are key drivers of innovation.

Misalignment with the EU Regulatory Approach

By adopting the EU Artificial Intelligence Act (AI Act), the European Union established a comprehensive regulatory framework based primarily on risk management, transparency, human oversight, and the respective obligations of the various actors involved throughout the lifecycle of an AI system.

The aim of this approach is not to penalize the technology itself, but to prevent harm through risk assessments, technical and organizational safeguards, market surveillance and regulatory enforcement. In other words, the emphasis is on prevention and risk management before harmful consequences arise. Criminal law, by contrast, remains a measure of last resort for the most serious cases.

A similar approach can be seen in other European initiatives, including the Product Liability Directive. The European Commission seeks to address liability for damage caused by AI primarily through civil law and regulatory mechanisms, including product liability and compensation rules, rather than by creating new general criminal offenses relating to artificial intelligence. The objective is to strike an appropriate balance between protecting individuals and fostering technological innovation.

Broader European Approaches

Comparative practice also shows that most countries give priority to regulatory, civil law and administrative liability mechanisms, while criminal law is generally reserved for specific and clearly defined forms of misuse of technology. For example, in its policy paper *AI regulation: a pro-innovation approach*, the United Kingdom expressly advocates a proportionate and pro-innovation regulatory model, warning that an overly rigid approach could slow the adoption of AI and stifle innovation. Rather than establishing a single criminal law regime, the UK relies on sector-specific regulators, existing legal frameworks, and the gradual development of regulatory standards.[1] Similarly, Italy, which adopted a national artificial intelligence law in 2025, linked its criminal law provisions to specific forms of misuse, such as the unlawful dissemination of deepfake content, fraud, or identity theft, rather than to the general concept of "causing danger" during the development or deployment of AI systems.[2]

[1] Available at: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach Accessed on 2 June 2026
[2] Available at: https://www.nortonrosefulbright.com/en/knowledge/publications/9bfedfea/italy-enacts-law-no-132-2025-on-artificial-intelligence-sector-rules-and-next-steps Accessed on June 2, 2026

Likewise, France[3], Germany[4] and the United Kingdom[5] have criminalized, or indicated their intention to criminalize, the unauthorized creation and distribution of sexually explicit deepfakes – digitally fabricated sexual content that may or may not be generated using AI – in order to protect privacy, personality rights, and human dignity. Such content is increasingly classified as a form of sexual violence, and European legislative developments are moving towards its criminalization through national criminal law provisions or through the implementation of the EU Directive on combating violence against women and domestic violence[6].

International Practice

Outside Europe, the prevailing approach is likewise to regulate AI primarily through principles of accountability, risk management, and technical standards, rather than through broad criminal prohibitions.

The OECD AI Principles, updated in 2024, emphasize the accountability of AI actors, risk management, and proportionality based on the actor's role and the context in which AI is used[7]. Similarly, the UNESCO Recommendation on the Ethics of Artificial Intelligence is grounded in human rights, transparency, human oversight, accountability, and the rule of law[8].

In the United States, at least at the federal level and in the area of general AI governance, an important point of reference is the *NIST AI Risk Management Framework*. It is expressly designed as a voluntary tool to help organizations manage AI-related risks and enhance the trustworthiness of AI systems. This further illustrates the international tendency to regulate AI primarily through standards, processes, and risk management, rather than through standalone criminal offenses of general application[9].

South Korea provides an example of one of the world's strictest regimes for combating deepfakes. Notably, even the possession or viewing of nonconsensual pornographic deepfake content constitutes a criminal offense (punishable by imprisonment or a fine). The legislation also establishes mandatory minimum sentences: at least one year of imprisonment for blackmail involving deepfake content and at least three years of imprisonment for creating sexually explicit deepfakes with the intent to distribute them. In addition, the state is required to assist victims in removing deepfake content from the internet[10].

Against this background, the Croatian approach may be regarded as more stringent than the prevailing European and international trends, which seek to strike a balance between protecting citizens and fostering innovation while reserving criminal law as a measure of last resort for the most serious forms of misuse. Article 215a departs from this approach by introducing a separate criminal offense of causing danger through the use of an AI system, carrying penalties of up to 15 years' imprisonment where the offense results in death. This sets artificial intelligence apart from the EU's general regulatory approach and subjects it to a stricter criminal law regime.

AmCham Recommendations

AmCham supports the existence of effective mechanisms to protect against the harmful and irresponsible use of artificial intelligence. However, we believe there is scope to further improve the current framework in order to provide greater legal certainty and predictability and bring it more closely into line with the European regulatory approach. In particular, it is essential to ensure that the scope of criminal liability is clearly defined and proportionate to the severity of the sanctions prescribed by law. This would reduce regulatory uncertainty and create an environment that both protects the public and encourages innovation.

[3]Available at: https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes Accessed on: June 1, 2026
[4]Available at: https://www.gesetze-im-internet.de/stgb/__201a.html Accessed on: June 1, 2026
[5]Available at: https://www.mishcon.com/news/government-to-criminalise-the-creation-of-sexually-explicit-deepfakes Accessed on: June 3, 2026
[6]Available at: https://ceeddw.org/wp-content/uploads/2025/05/NCII_DeepFakes_ThreatsRecommendations.pdf Accessed on: June 3, 2026
[7] Available at: https://www.oecd.org/en/topics/sub-issues/ai-principles.html Accessed on: June 8, 2026
[8] Available on: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics Accessed on: June 8, 2026
[9] Available at: https://www.nist.gov/itl/ai-risk-management-framework Accessed on: June 3, 2026
[10] Available at: https://ondato.com/blog/deepfake-laws Accessed on: June 3, 2026

1) Introducing a Blanket Criminal Provision

One possible way to address the shortcomings identified above would be to reformulate the provision as a blanket criminal provision. In criminal law, blanket provisions refer to other legislation that regulates a particular area in greater detail, thereby providing greater flexibility and ensuring that criminal law remains aligned with technical and regulatory standards. In the context of AI, such a provision could refer to relevant European and national legislation, in particular the obligations arising under the EU AI Act, technical standards governing system safety, risk-assessment obligations, and human oversight requirements applicable to high-risk systems.

For example, criminal liability could be connected to situations in which a person intentionally breaches prescribed safety obligations relating to the development or deployment of high-risk AI systems and that breach results in serious danger or harmful consequences for life, health, or property. This would focus criminal law on breaches of specific legal obligations rather than on the abstract concept of causing danger.

- ***Recommendation:***
  Introduce a blanket criminal law provision that clearly links criminal liability to specific breaches of safety and regulatory obligations established under European and national legislation governing the use of AI systems.

2) Defining the Scope More Precisely

AmCham believes that criminal liability should be linked more precisely to specific consequences caused by the use of AI. Instead of relying on the general concept of "causing danger", we propose defining a narrower set of circumstances in which criminal liability would arise. For example, where AI is used in a manner that results in serious breaches of safety or security, the manipulation of information with severe societal consequences, endangerment of critical infrastructure, or other forms of harm. Such an approach has already been adopted in certain European jurisdictions, where criminal law is applied primarily to specific forms of technological misuse, such as serious fraud or identity manipulation through deepfakes.

AmCham supports the responsible use of AI and recognizes the need to sanction serious forms of misuse. However, we believe that the criminal law framework must be sufficiently clear, predictable, and aligned with the European regulatory approach to protect the public while fostering innovation. Defining the boundaries of criminal liability more clearly and linking them to specific regulatory obligations would contribute to a stable environment for the development and deployment of artificial intelligence in Croatia and support economic growth.

- ***Recommendation:***
  Limit criminal liability more precisely to clearly defined and particularly harmful forms of AI misuse, such as identity manipulation, serious fraud, and endangerment of critical infrastructure.

3) Applying the Principles of Proportionality and Graduated Liability

AmCham recommends drawing a clearer distinction between regulatory, civil, and criminal forms of liability, with criminal law being applied primarily to the most serious and intentional forms of AI misuse.

The majority of European and international regulatory frameworks address issues relating to AI systems primarily through risk management, regulatory oversight, administrative measures, and civil liability for harm, while criminal law is used as a measure of last resort for particularly dangerous or intentional conduct. Such an approach provides effective protection for the public while providing greater legal certainty for organizations that develop and use AI systems.

- ***Recommendation:***
  Apply criminal law primarily to the most serious and intentional forms of AI misuse, while addressing other risks through regulatory and civil law mechanisms in accordance with international practice.

For additional information, please contact: American Chamber of Commerce in Croatia

Andrea Doko Jelušić | Executive Director

T: 01 4836 777 | E: andrea.doko@amcham.hr