



## CRIMINAL LIABILITY FOR HARM CAUSED BY ARTIFICIAL INTELLIGENCE SYSTEMS: CROATIAN LEGAL REFORM AND THE EU LAW CONTEXT

**Vedran Kruljac, PhD, Lecturer**

University North, University Center Varaždin  
Jurja Križanića 31b, 42000 Varaždin, Croatia  
vkruljac@unin.hr

**Sunčana Roksandić, PhD, Associate Professor**

University of Zagreb, Faculty of Law  
Trg Republike Hrvatske 14, 10000 Zagreb, Croatia  
suncana.roksandic@pravo.hr

**Doris Skaramuca, PhD student, Junior Researcher**

University of Miskolc, Deák Ferenc Doctoral School of Law; Central European Academy  
Városmajor u. 12-14., 1122 Budapest, Hungary  
doris.skaramuca@centraleuropeanacademy.hu

### ABSTRACT

*The rapid deployment of artificial intelligence (AI) systems across the European Union (EU) raises profound legal challenges, particularly regarding liability for damage caused by autonomous or semi-autonomous systems. While AI promises significant economic and societal benefits, its increasing autonomy disrupts traditional legal concepts of fault, causation, and responsibility. This tension is clearly illustrated by recent national debates, such as in Croatia, where proposals have emerged to introduce criminal liability for harm caused by AI systems, resulting in new criminal offence introduced in 2025, despite unresolved questions concerning the identification of the responsible legal subject. At the EU level, policymakers have sought to address these challenges through a comprehensive regulatory framework, most notably the Artificial Intelligence Act (AI Act) and the proposed reforms of civil liability rules for defective products and emerging digital technologies. These instruments aim to balance innovation with legal certainty, risk management, and the protection of fundamental rights. However, they*

*predominantly focus on ex ante risk regulation and civil liability mechanisms, leaving unresolved issues regarding criminal liability and the attribution of responsibility in cases involving complex AI-driven decision-making processes.*

*This paper examines the evolving EU approach to liability for AI-caused damage and assesses its implications for legal certainty within member states. The research focuses on three core questions: (1) how EU law conceptualizes responsibility and accountability for AI-related harm; (2) how national legal systems, using Croatia as a case study, attempt to transpose or supplement EU norms through criminal and civil law instruments; and (3) whether existing regulatory models adequately address the practical and normative challenges posed by autonomous AI systems.*

*Methodologically, the paper employs doctrinal legal analysis of EU legislation and policy documents, comparative examination of national legal approaches, and critical review of relevant academic literature. Where available, emerging judicial reasoning and analogies from existing case law on technological risk and product liability are also considered.*

*The paper argues that current regulatory developments reveal a fragmented approach to AI liability that risks undermining legal certainty and uniform application of EU law. It concludes by proposing normative guidelines for a more coherent EU-wide framework that clarifies the attribution of responsibility, enhances harmonization across member states, and strengthens the EU's role as a global standard-setter in AI governance.*

**Keywords:** *AI-caused harm, Artificial intelligence, Criminal liability, EU law, Legal certainty*

## 1. INTRODUCTION

The accelerated development and increasingly widespread deployment of AI over the past decade have profoundly transformed social, economic, and legal relations. Autonomous and semi-autonomous systems are now used, for example, in transport, healthcare, financial services, industry, and public administration, where their decisions may have direct and significant consequences for individuals' lives, health, and property.

The increasing use of machine learning systems and advanced algorithms means that certain decisions are no longer made exclusively by human actors, but emerge from complex technical processes whose outcomes may be difficult to predict. This unpredictability may give rise to risks for fundamental rights and human dignity.<sup>1</sup>

At the EU level, the adoption of the AI Act<sup>2</sup> has established a comprehensive regulatory framework based on a risk-based approach. Criminal liability for harm or

<sup>1</sup> Roksandić, S.; Protrka, N.; Engelhart, M., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?*, IEEE, 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), 2022, p. 1400.

<sup>2</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU)

risk caused by AI is not harmonised at the EU level and remains within the competence of the Member States. This is a consequence of the absence of EU competence in criminal law harmonisation within the EU legal order, under which national legal systems retain responsibility for defining the conditions of criminal liability.

Criminal law traditionally rests on the concepts of individual culpability, unlawfulness, and personal responsibility. It presupposes human conduct and a mental element on the part of the perpetrator in relation to the offence (intent or negligence), on the basis of which blame may be attributed. The criminal liability of legal persons is grounded in acts or omissions, as well as in failures of supervision by responsible persons.<sup>3</sup>

In the context of AI, these concepts are confronted with significant challenges. Where an autonomous system causes harm or creates a risk, the question arises as to whom, and under what conditions, criminal responsibility should be attributed: the programmer, the manufacturer, the distributor, the operator, or the end user?<sup>4</sup>

Complex causal chains and the technical opacity of algorithms (“black box” systems) complicate both the establishment of causation and the assessment of the mental element. This paper proceeds from the premise that existing criminal law doctrines can be applied to such situations, but require careful and restrictive interpretation. At the same time, the application of these doctrines must respect the fundamental limits of criminal law, particularly the principle of legality and the prohibition of objective liability.

---

No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] OJ L2024/1689 (Artificial Intelligence Act) (Text with EEA relevance).

<sup>3</sup> Pursuant to Art. 3 para. 2 of the Act on the Liability of Legal Persons for Criminal Offences (Croatia), Official Gazette No. 151/03, 110/07, 45/11, 143/12, 114/22, 114/23, a legal person shall be punished for a criminal offence committed by a responsible person where, by such offence, a duty of the legal person is violated or the legal person has obtained or was intended to obtain a benefit for itself or for another. See in: Dragičević Prtenjača, M.; Roksandić, S., *Criminal Law and Criminal Compliance in Croatia*, in: Papathanasiou, K. (ed.), *Corporate Criminal Law and Criminal Compliance*, Vienna, 2023, pp. 137–164. Under the aforementioned conditions, a legal person shall be punished for a criminal offence committed by a responsible person entrusted with the performance of tasks within the scope of the legal person's activities, where the offence was committed as a result of a failure of supervision or control by a responsible person managing the affairs of the legal person. Under the same conditions, a legal person shall be punished for criminal offences prescribed by the Criminal Code and by other statutes providing for criminal offences.

<sup>4</sup> Roksandić Vidlička, S.; Liepiņa, E.; Ostapchuk, S., *Bioethical and Legal Challenges of Artificial Intelligence and Human Dignity*, in: Jovanović, M.; Virady, Tibor (eds.), *Human Rights in 21st Century*, Netherlands, 2020, pp. 269–288.

In such a normative context, the Croatian legislator amended the Criminal Code in 2025, introducing a statutory definition of an “AI system” and a new criminal offence of endangering life and property through the use of an AI system.<sup>5</sup> The new criminal offence (Article 215a of the Criminal Code/11) encompasses persons involved in the development, testing, validation, placing on the market, supervision, management, or use of AI systems, or otherwise involved, where, through their conduct, a danger is created to life, bodily integrity, or property of a large scale, with aggravated forms provided for in cases of serious bodily injury or death, or large-scale property damage.<sup>6</sup>

However, such an innovation raises a number of questions. To what extent is the definition of an AI system aligned with European law? Are the constituent elements of the criminal offence formulated with sufficient precision to satisfy the principle of legality, in particular the requirement of *nullum crimen sine lege certa*? A particularly sensitive issue concerns the degree of guilt, especially the distinction between intent and negligence and the risk of expanding liability towards objective responsibility. In this context, it is necessary to clarify whether negligence relates to the conduct itself or only to the resulting consequence, and how Croatian law positions this distinction in comparative perspective.

In light of the foregoing, this paper pursues a threefold objective. This paper argues that AI-related criminal liability does not require new categories of guilt, but a restrictive reinterpretation of existing doctrines, particularly negligence and organisational fault.

First, to provide a systematic analysis of the new criminal offence and the definitions related to AI in Croatian criminal law, including an examination of issues of causation, objective imputation, guilt, and the liability of legal persons. Second, to assess the Croatian solution from a comparative perspective in light of EU law, taking into account the broader EU regulatory framework and its interaction with national criminal law. Third, to identify legal uncertainties and challenges concerning the attribution of responsibility, as well as the distinction between criminal and civil liability in this field.

The analysis is guided by the following research questions: (1) whether the statutory definition of AI ensures sufficient clarity and alignment with the European framework; (2) whether the constituent elements of the new criminal offence sat-

---

<sup>5</sup> Art. 87 para. 33 and art. 215.a of the Criminal Code (Croatia), Official Gazette No. 144/2012, 125/2011, 56/2015, 61/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022, 114/2023, 36/2024, 136/2025.

<sup>6</sup> Criminal Code (Croatia), Art. 87 para. 27.

isfy the requirements of legality, foreseeability, and precision; (3) how classical doctrines of criminal law, in particular causation and negligence, can be applied in the context of autonomous systems; and (4) how the relationship between criminal and civil liability should be understood in this field. In doing so, the paper positions itself against approaches that advocate the creation of new categories of criminal liability for AI, arguing instead for doctrinal continuity combined with interpretative adjustment.

Methodologically, the paper is based on a doctrinal analysis of positive law, a structured comparative legal analysis, and a critical review of the relevant literature. The paper argues that, while the Croatian reform represents an important step towards addressing AI-related risks, its application requires a restrictive interpretation of statutory elements and a clearer doctrinal distinction between different forms of fault in order to preserve the principles of legality and personal guilt.

## 2. THE REGULATORY EU FRAMEWORK

### 2.1. Constitutional Context and Regulatory Purpose of the AI Act

The subsequent sections of the paper analyse criminal and civil liability for AI, with the EU regulatory framework providing the key background to recent reforms and legal debates. This section provides a structured overview of the AI Act, its regulatory logic, and its relationship to national systems of liability. For the purposes of this paper, the relevance of the EU framework lies primarily in its impact on national legal systems, particularly in shaping regulatory obligations that may be relevant for the assessment of criminal liability.<sup>7</sup>

The AI Act constitutes the first comprehensive European regulatory framework that approaches AI through a risk-based framework. It categorises AI systems into four levels of risk – “unacceptable risk (prohibited)”<sup>8</sup>, “high risk (regulated)”<sup>9</sup>, “limited risk (transparency)”<sup>10</sup>, and “minimal/no risk (unregulated)” – and lays down corresponding obligations for providers and operators of such systems.

From the recitals of the AI Act it follows that the existing EU legal framework is not sufficient to address the specific risks generated by AI systems, which necessitated the establishment of a uniform horizontal regulatory framework. The

<sup>7</sup> Kritikos, M., *Artificial Intelligence ante portas: Legal & ethical reflections*, 2019, Available at: [[https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634427/EPRS\\_BRI\(2019\)634427\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634427/EPRS_BRI(2019)634427_EN.pdf)], Accessed 26 March 2026.

<sup>8</sup> Art. 5 of the AI Act.

<sup>9</sup> Art. 6-27 of the AI Act.

<sup>10</sup> Art. 50 of the AI Act.

Regulation is therefore conceived as a response to regulatory gaps, in particular with the aim of ensuring a high level of protection of fundamental rights, safety, and health.

## 2.2. Preventive regulatory model and limits of EU competence

In this regard, AI systems presenting an unacceptable risk (e.g. manipulation, social scoring, profiling for the purpose of predicting criminal behaviour) are explicitly prohibited. High-risk AI systems may be placed on the market only subject to strict safety and oversight mechanisms, while transparency and supervision are expressly prescribed for general-purpose AI models, including requirements to inform users when they are interacting with AI.<sup>11</sup>

The AI Act builds upon existing product safety mechanisms, extending them to address AI as a horizontal technology across multiple sectors.<sup>12</sup> Its primary function is preventive (*ex ante*), while liability remains governed by separate instruments and national law. This structural separation between *ex ante* regulation and *ex post* liability contributes to legal fragmentation, particularly in areas where technological complexity challenges traditional doctrines of attribution.

## 2.3. Civil Liability Developments at the EU Level

Although the AI Act defines risks, the approach to liability at the EU level remains uneven. Two principal directions can be identified in the field of civil liability: the proposed AI Liability Directive and the reformed regime of liability for defective products.

In 2022, the European Commission proposed the Artificial Intelligence Liability Directive (AILD) with the aim of modernising the rules on liability for damage caused by AI systems. Under this initiative, the AILD would introduce a rebuttable presumption of causation in order to alleviate the burden of proof for victims seeking to establish damage caused by an AI system.<sup>13</sup>

<sup>11</sup> Art. 51-56 of the AI Act. In the context of explainability and transparency, see in: High Level Expert Group on Artificial intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI*, 2019, Available at: [<https://www.aepd.es/sites/default/files/2019-12/aiethics-guidelines.pdf>], Accessed 26 March 2026.

<sup>12</sup> Lewis, D. *et al.*, *Mapping the Regulatory Learning Space for the EU AI Act*, arXiv, 2025, Available at: [<https://arxiv.org/html/2503.05787v2>], Accessed 10 January 2026.

<sup>13</sup> European Parliament, *Artificial Intelligence Liability Directive*, 2025, Available at: [<https://arxiv.org/html/2503.05787v2>], Accessed 11 January 2026.

Its withdrawal in 2025 reflects the practical and political difficulties of harmonising civil liability within the EU legal order.<sup>14</sup> The withdrawal also illustrates the limits of consensus among Member States in balancing innovation, competitiveness, and the protection of injured parties.

In addition to the directive specifically dedicated to AI, under the Revised Product Liability Directive the concept of “product” has been expanded to include software and AI systems<sup>15</sup>, thereby extending the EU legal framework for liability for defective products to encompass digital and software-intensive technologies that are increasingly present on the market. This reformed system of civil liability reflects the growing importance of software and AI within complex value chains, while maintaining that liability is attributed to the relevant economic operators involved in their development and deployment.

In this way, civil liability is broadened to encompass autonomous digital systems, while remaining distinct in its function and doctrinal foundations from criminal liability. However, questions remain as to whether the concept of “defectiveness” can fully capture damage resulting from the autonomous behaviour of learning systems.

#### **2.4. Case Law and Indirect Relevance for Criminal Liability**

To date, there are no judgments of the Court of Justice of the European Union (CJEU) that directly address criminal liability in relation to AI. This reflects the limited competence of the EU in criminal law matters. Nevertheless, there are cases concerning digital technologies and liability in EU law more generally, in which the CJEU has addressed liability in the context of digital services and data processing, albeit not on the basis of the AI Act.

The Court has held that operators of online platforms and search engines may incur liability where their role goes beyond that of a neutral intermediary and involves a degree of control over content or data processing.<sup>16</sup> Although these decisions were not adopted on the basis of the AI Act, they establish an interpretative

<sup>14</sup> Euronews, *EU Tech Commissioner defends scrapping of AI Liability rules*, 2025, Available at: [<https://arxiv.org/html/2503.05787v2>], Accessed 12 January 2026.

<sup>15</sup> P. 3 and 6 of the Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L, 2024/2853 (Text with EEA relevance).

<sup>16</sup> Case C-492/23 – Russmedia Digital SRL and Inform Media Press SRL [2025] ECLI:EU:C:2025:935, pp. 106 and 126. Case C-131/12 Google Spain SL and Mario Costeja González [2014] 2012/C 165/18, pp. 33 and 38.

framework that may influence the understanding of liability in technologically complex environments.<sup>17</sup>

Several conclusions follow from the foregoing. First, the European regulatory approach to AI is primarily preventive and risk-based. Second, the AI Act does not harmonise liability, but operates alongside civil law instruments and national legal systems. Third, there is a recognised need to adapt certain legal doctrines, particularly with regard to evidence and standards of fault, in order to address the specific challenges posed by AI systems. EU law therefore does not directly regulate criminal liability, but may influence its interpretation indirectly through general principles such as legal certainty and proportionality.

## 2.5. Synthesis: multi-level liability framework

The European model of AI regulation is primarily based on prevention and risk management, while issues of liability are addressed through a combination of civil law instruments and national legal systems. From a criminal law perspective, this creates a structural gap: regulatory obligations are harmonised at the EU level, while the attribution of criminal responsibility remains fragmented and dependent on national legal doctrines. In this context, the Croatian reform represents an attempt to address risks that are otherwise regulated at the EU level primarily through preventive mechanisms.

## 3. CRIMINAL LAW REGULATION OF ARTIFICIAL INTELLIGENCE IN CROATIA

Through the amendments to the Criminal Code of 2025<sup>18</sup> the Croatian legislator has, for the first time, expressly introduced criminal law regulation of AI. This intervention represents a specific legislative response to risks associated with technologically complex and adaptive systems, rather than a departure from existing criminal law structures.

<sup>17</sup> Charter of Fundamental Rights of the European Union [2012] OJ C 326/391. See also in: Wagner, G., *Liability Rules for the Digital Age – Aiming for the Brussels Effect*, Journal of European Tort Law, Vol. 13, Issue 3, 2023, p. 191. See also in: Rodríguez de Las Heras Balle, T., *Mapping Generative AI rules and liability scenarios in the AI Act, and in the proposed EU liability rules for AI liability*, Cambridge Forum on AI: Law and Governance, Vol. 1, Issue e5, 2025, p. 2. See also in: Ebers, M. *et al.*, *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, J, Vol. 4, Issue 4, 2021, p. 601. See also in: Novelli, C. *et al.*, *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*, Computer Law & Security Review, Vol. 55, 106066, 2024, p. 1. See also in: Tran, H. C., *Unbounded Harms, Bounded Law: Liability in the Age of Borderless AI*, J, arXiv preprint arXiv:2601.12646, 2026, p. 1.

<sup>18</sup> Amendments to the Criminal Code (Croatia), Official Gazette No. 136/2025.

This legislative reform encompasses two fundamental elements: (1) the introduction of a statutory definition of an “AI system” into the Criminal Code/11<sup>19</sup> and (2) the introduction of a new criminal offence of endangering life and property through the use of an AI system.<sup>20</sup> The legislator has thus combined a technologically neutral definition with a specific incrimination. While this approach ensures flexibility, it also requires a restrictive interpretation in order to comply with the principle of legality.

The definition of an AI system in the Croatian Criminal Code is substantively aligned with the definition set out in the AI Act, under which ‘AI system’ means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.<sup>21</sup>

By adopting a functional and technologically neutral definition, the legislator has ensured compatibility with European law and alignment with the broader regulatory framework. However, from a criminal law perspective, the key issue is the precision of the provision set out in Article 215a of the Criminal Code.

The Croatian criminal law intervention must be understood in the context of the EU regulatory framework, which is primarily preventive and does not regulate criminal liability, and focuses on risk classification, obligations of providers and users, and systems of oversight. This legislative intervention differs from classical forms of technological regulation in that AI is not treated merely as an instrument, but as a source of risk arising from its design, deployment, and use.

Such an approach raises the question of the limits of criminal law in regulating AI systems whose full effects may only become apparent *ex post*. In this respect, criminal law must avoid extending liability beyond the boundaries of personal culpability, as doing so would risk transforming fault-based responsibility into de facto objective liability.

<sup>19</sup> Amendments to the Criminal Code (Croatia), Art. 87 para. 33 of the Criminal Code (Croatia).

<sup>20</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] OJ L2024/1689 (Artificial Intelligence Act) (Text with EEA relevance).

<sup>21</sup> Compare Art. 3 para. 1 of the AI Act with Art. 87 para. 33 of the Criminal Code (Croatia).

From a systematic perspective, the new criminal offence is placed among offences against public safety of persons and property. The legislator thus treats AI as a source of technological risk.

Unlike classical sources of danger, AI does not possess inherent physical hazardousness; the relevant risk arises from human decisions in its design, configuration, and use. At the same time, their adaptive and complex behaviour justifies specific regulatory attention.

From a doctrinal perspective, this constitutes an endangerment offence. The basic form of the offence is completed already by the creation of a concrete danger to protected legal goods (life or bodily integrity of persons, or property of a larger scale), while serious bodily injury or death, as well as large-scale property damage, are provided for as aggravated forms. This confirms the preventive character of the offence. However, extending punishability to the stage of concrete endangerment requires a restrictive interpretation, ensuring that only real and individualised risks fall within the scope of criminal liability.

The principle of *ultima ratio* requires that criminal law be applied only where other branches of law are insufficient to protect fundamental legal goods. Accordingly, broadly formulated elements of the offence, such as “or otherwise”, must be interpreted restrictively in line with the principle of legality.<sup>22</sup>

The *actus reus* of the criminal offence of endangering life and property through the use of an AI system encompasses the development, testing, validation, placing on the market, supervision, management, and use of AI systems, or otherwise the use of an AI system. Such a broad formulation covers the entire life cycle of the technology. This indicates that responsibility may extend beyond the end user to other actors involved in the life cycle of the system.

In this context, it is also necessary to consider the relationship between this offence and other criminal offences. Where, in addition to endangerment, actual harm occurs (e.g. bodily injury or death), issues of concurrence arise. In principle, the rules on concurrence require an assessment of whether the conduct constitutes a single offence with aggravated consequences or multiple offences in real concurrence. This depends on the specific circumstances of the case and the structure of the statutory provisions.

Such breadth requires a clear distinction between regulatory non-compliance, professional error, and criminally relevant conduct. The objective element of this

<sup>22</sup> Art. 1 of the Criminal Code (Croatia). Novoselec, P. (ed.), *Posebni dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2007, pp. 505-524. See also in: Vuletić, I., *Corporate Criminal Liability: An Overview of the Croatian Model after 20 Years of Practice*, Laws, Vol. 12, Issue 2, 2023, Article 27, pp. 2-5.

criminal offence consists in creating a danger to the life or bodily integrity of persons, or to property of a larger scale. In this respect, it is crucial to emphasise the distinction between abstract and concrete danger.

For the application of Article 215a, the danger must be concrete and individualised, rather than merely hypothetical. Croatian case law requires that courts establish the individual responsibility of the accused and the existence of a concrete danger, ensuring that liability is not attributed in abstract terms.<sup>23</sup>

In the AI context, this requires an assessment of whether a specific configuration or use of the system created a foreseeable and preventable risk. As regards causation, it exists where the conduct of the perpetrator, according to the rules of experience and the laws of nature, was capable of bringing about the resulting consequence, and where that consequence is not the result of extraordinary and unforeseeable circumstances. In the context of AI systems, the notion of unforeseeable circumstances is particularly relevant, given the potential for complex and adaptive behaviour. A mechanical attribution of all system errors to developers or operators would disregard the complexity of such systems.

However, the application of these criteria is particularly complex in technologically sophisticated environments. These difficulties may be illustrated by the example of an autonomous vehicle that fails to recognise a pedestrian due to limitations in training data and specific environmental conditions, resulting in serious bodily injury.

In such a case, the key legal question is whether a specific actor breached a duty of care in a manner that created a foreseeable and preventable risk. For example, liability may arise if the developer failed to address known limitations of the system, or if the operator deployed the system in conditions for which it was not intended. Conversely, where the system operates within expected parameters and the outcome is not foreseeable, criminal liability should be excluded.

In such circumstances, multiple potential addressees of the norm come into consideration, including the vehicle manufacturer, the developer of the AI system, the entity responsible for maintenance and updates, as well as the user or operator.<sup>24</sup>

<sup>23</sup> Judgement of the Supreme Court of the Republic of Croatia No. I Kž 438/2018-11 of 21 October 2020. Judgement of the Supreme Court of the Republic of Croatia No. I Kž 561/2020-9 of 15 April 2021. Dragičević Prtenjača, M.; Roksandić, S., *op. cit.*, note 3, pp. 137–164. See also in: Law on the Liability of Legal Persons for Criminal Offences (Croatia).

<sup>24</sup> Gless, S.; Silverman, E.; Weigend, T., *If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability*, New Criminal Law Review, Vol. 19, Issue 3, 2016, p. 412. See also in: Roksandić Vidlička, S.; Liepiņa, E.; Ostapchuk, S., *op. cit.*, note 4, pp. 270–272.

However, the mere occurrence of harm is not sufficient to establish criminal liability; it must be shown that a concrete and individualised danger is linked to a breach of a duty of care by a specific person.<sup>25</sup>

Where the system operates within its intended parameters and the outcome is objectively unforeseeable, negligence may be excluded. Conversely, disregard of known limitations or failures of supervision and control may constitute a breach of the duty of care. In such cases, liability may arise for both individuals and legal persons, where the offence results from failures in supervision or control.<sup>26</sup>

By contrast, different hypothetical constellations may lead to different attributions of liability. For instance, if a developer knowingly deploys an AI system despite documented deficiencies in its training data, liability may arise at the development stage.

If an operator uses a system in conditions explicitly excluded by its design specifications, liability may arise at the level of use. Finally, where a company systematically fails to implement adequate monitoring and compliance mechanisms, liability may arise on the basis of organisational fault.

The diffusion of decision-making characteristic of AI systems complicates the attribution of individual responsibility, particularly in complex organisational structures involving multiple actors. This makes the requirement of individualisation of liability particularly important, as criminal responsibility cannot be inferred from systemic failure alone without identifying a concrete breach of duty by a specific actor. Criminal liability must nevertheless remain individualised and linked to a concrete contribution and a breach of duty in relation to a foreseeable risk, in accordance with the principle of legality and the requirement of foreseeability of criminal liability.<sup>27</sup>

In Croatian criminal law, it is necessary to distinguish clearly between intent and negligence. Intent presupposes awareness and acceptance of the prohibited consequence, whereas negligence is characterised by a lack of such acceptance, even where the consequence was foreseeable.

<sup>25</sup> Novokmet, A.; Roksandić, S.; Vidaković I., *Tehnološki potaknute promjene u kaznenom postupku: održavanje ravnoteže učinkovitosti kaznenog postupka i prava na obranu*, in: Modernizacija prava, Knjiga 82., Regulacija umjetne inteligencije u Europskoj uniji: Tehnološki izazovi i etička pitanja, pp. 63-98.

<sup>26</sup> Marchant, G. E.; Lindor, R. A., *The Coming Collision Between Autonomous Vehicles and the Liability System*, Santa Clara Law Review, Vol. 52, Issue 4, 2012, p. 1321. Art. 3 p. 2 of Law on the Liability of Legal Persons for Criminal Offences (Croatia).

<sup>27</sup> Art. 7 of the Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, E.T.S. No. 5, 213 U.N.T.S. 222. Art. 49 of the Charter of Fundamental Rights of the European Union. *Kokkinakis v Greece* (1993) 52 ECHR 20. *Cantoni v France* (1996) 35 ECHR 121.

In this respect, the concept of negligence may differ from certain comparative approaches in which awareness of risk combined with acceptance may be classified as intent. Negligence exists where the perpetrator was obliged and able to foresee the possibility of the harmful consequence but failed to exercise due care.

In comparative criminal law, particularly in systems recognising *dolus eventualis*, awareness of a risk combined with acceptance of its occurrence may qualify as intent rather than negligence. However, Croatian law maintains a stricter distinction, requiring acceptance of the consequence for intent, whereas mere awareness without acceptance remains within the scope of negligence. In this respect, it is important to clarify that negligence in Croatian criminal law may relate both to the conduct and to the resulting consequence; however, in the analysed offence, it is primarily linked to the failure to prevent a foreseeable and avoidable consequence, rather than to the mere performance of the act itself.

The analysed offence is primarily structured as a negligent offence. Intentional commission would require that the perpetrator was aware that their conduct would create a concrete danger and accepted such an outcome, which, in the context of AI systems, is expected to be exceptional.

Accordingly, the doctrinal construction of the offence must be understood as centred on negligence, particularly in relation to the resulting danger. From a doctrinal perspective, intentional commission of this offence is not excluded, but would require a situation in which the perpetrator is aware that their conduct creates a concrete danger and nevertheless accepts such an outcome, which in practice will occur only in exceptional circumstances.

While civil liability primarily serves a reparative function, criminal liability is based on the attribution of personal guilt. Although both may rely on the concept of negligence, their content is not identical. Criminal negligence requires a higher degree of fault and is subject to stricter standards of proof, reflecting the punitive nature of criminal law.<sup>28</sup>

This implies that omissions may constitute a relevant form of conduct under Croatian criminal law. In particular, failures to implement adequate supervision, monitoring, or risk management measures may give rise to liability where a legal duty to act exists. Since approaches to omission differ across legal systems, it is important to emphasise that Croatian law recognises omission as a basis of criminal liability where a specific duty of care is established.

---

<sup>28</sup> Art. 41 of the Criminal Code (Croatia).

Under Croatian criminal law, such duties may arise from statutory provisions, contractual obligations, or the assumption of responsibility within organisational structures. In the context of AI systems, this is particularly relevant for actors responsible for supervision, monitoring, and risk management throughout the lifecycle of the system.

The relevance of fundamental rights must be interpreted cautiously, as their horizontal effect remains debated.<sup>29</sup> In this context, their relevance in criminal law does not stem from direct horizontal applicability, but rather from their interpretative function in shaping the content of legal duties and standards of care, particularly where regulatory obligations under EU law inform the assessment of unlawfulness. The principle of proportionality requires that penalties correspond to the gravity of the offence and the degree of guilt.<sup>30</sup>

Even where AI is involved, criminal liability remains attached to natural or legal persons.<sup>31</sup> The Croatian reform represents an important step in addressing AI-related risks, but its effectiveness depends on a restrictive and doctrinally consistent interpretation of its elements, particularly with regard to negligence, omission, and the requirement of individualised criminal liability.<sup>32</sup>

#### 4. COMPARATIVE AND NORMATIVE ANALYSIS

A comparative analysis of criminal law regulation of AI in the Member States of the EU reveals significant normative diversity, while confirming a shared conceptual core: the preservation of the anthropocentric structure of criminal law. Accordingly, notwithstanding technological innovations and the increasing au-

<sup>29</sup> Art. 1, 7 and 8 of the Charter of Fundamental Rights of the European Union. Moch, E., *Autonomous Systems (AI) and Criminal Imputability: Challenges for Modern Law*, International Journal of Research and Review, Vol. 12, Issue 10, 2025, p. 290.

<sup>30</sup> Art. 49 para. 3 of the Charter of Fundamental Rights of the European Union.

<sup>31</sup> Berdica, J.; Herceg Pakšić, B., *Umjetna inteligencija i odabrani aspekti kaznenoga prava. O nekim izazovima za suvremenu pravnu kulturu*, Filozofska istraživanja, Vol. 42, Issue 1, 2022, p. 101. Mrčela, M.; Vuletić, I., *Novo kazneno djelo – dovođenje u opasnost života i imovine sustavom umjetne inteligencije*, Državno odvjetništvo otvara razgovor: DOOR, Vol. 1, Issue 1, 2025, p. 229.

<sup>32</sup> Vuletić, I.; Novokmet, A.; Tomićić, Z., *Izazovi posebnog dijela kaznenog prava zbog razvoja umjetne inteligencije uz poseban osvrt na hrvatsko kazneno pravo*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 47, Issue 1, 2024, p. 27. As regards the amendments in the regulation of criminal offences against the environment, in particular in accordance with the requirements of the Directive (EU) 2024/1203 of the European Parliament and of the Council of 11 April 2024 on the protection of the environment through criminal law and replacing Directives 2008/99/EC and 2009/123/EC [2024] OJ L, 2024/1203. See further in: Roksandić, S.; Engelhart, M., *Environmental Corruption: Fighting Two Evils through International Criminal Law Alongside Introducing a Special Protocol to UNCAC and UNTOC*, International Criminal Law Review, Vol. 25, Issue 2-3, 2025, pp. 247-270.

tonomy of algorithmic systems, only natural and legal persons – not AI systems – can be bearers of criminal liability.

The Croatian reform of 2025 introduced a specific criminal offence of endangering life and property through the use of an AI system, thereby representing a relatively innovative step in the European context. In doing so, the Croatian legislator has partially moved beyond the dominant model of relying exclusively on general criminal law doctrines and has normatively recognised the specificity of technologically generated risks.

Most EU Member States, by contrast, continue to rely on general criminal law doctrines without introducing AI-specific offences. For the purposes of comparison, the analysis focuses on the criminal liability of natural persons and, where relevant, the liability of legal persons based on organisational fault.

#### **4.1. Models Based on General Criminal Law (Germany, France)**

Germany has not introduced a specific criminal offence relating to AI; rather, liability is assessed under general offences such as negligent homicide and negligent bodily injury.<sup>33</sup> The German model is grounded in a strict doctrine of personal guilt, emphasising individual responsibility and rejecting any form of automated attribution of liability to a technological system.

AI is treated as a technical instrument, with liability depending on human intent or negligence. The system is analogous to a machine or vehicle and does not constitute a bearer of conduct in criminal law.

Nor does the French legal system contain an explicit provision criminalising AI-specific risks. Liability arises under general provisions relating to safety obligations of producers and distributors.

French law attributes liability to natural and legal persons, including for omissions, without recognising AI as a subject of liability.<sup>34</sup> Thus, causation may stem from software, but guilt is attributed to human or organisational failure.

<sup>33</sup> Art. 222 and 229 of the Criminal Code (Germany), in the version published on 13 November 1998 (Official Gazette I, p. 3322), as last amended by Article 2 (2) of the Act of 7 November 2024 (Official Gazette 2024 I No. 351).

<sup>34</sup> Art. 121-1 and 222-19 of the Criminal Code (France), in the version published on 29 July 1994 (Official Gazette No. 175), as last amended of the Act of 9 July 2025 (Official Gazette No. 622). See also in: Cartier M. E., *Kaznenopravna odgovornost pravnih osoba u francuskom pravu*, Hrvatski ljetopis za kazneno pravo i praksu, Vol. 12, Issue 2, 2005, pp. 279-293.

## 4.2. Organisational Liability Models (Italy, Spain)

Italy has followed an opposite path, initially proceeding with implementing national regulation. On 17 September 2025, the Italian Parliament approved the first national law on artificial intelligence, thereby making Italy the first country in the European Union to adopt domestic legislation governing the use of AI.<sup>35</sup>

Italy has a system of criminal liability of legal persons based on organisational fault.<sup>36</sup> Liability arises where effective compliance and risk-management systems are lacking. In the AI context, this includes failures in risk assessment, oversight, and internal controls.<sup>37</sup>

The criminal law reform of 2025 in Spain introduced a compliance-based approach where liability may be excluded if effective prevention mechanisms are in place.<sup>38</sup> This links criminal liability to organisational failure rather than technological risk alone.

## 4.3. Technologically Neutral Approaches (Netherlands, Austria)

Dutch law recognises criminal liability of legal persons (Article 51), but in practice liability is often attributed to natural persons within the organisation, in line with general criminal law principles. The Netherlands does not provide for AI-specific offences but applies existing offences, such as unlawful interference with data, to technologically mediated conduct.<sup>39</sup> This reflects a technologically neutral approach, allowing existing norms to be applied to AI systems.

In the AI context, liability may arise from failures to address known risks or from deficiencies in supervision. This approach enables adaptation to new technologies without introducing specific AI-related offences.

The Austrian model allows for the sanctioning of legal persons where a criminal offence is the result of failures in supervision or organisation.<sup>40</sup> In the AI sector, this may include inadequate validation of systems or the disregard of safety warn-

---

<sup>35</sup> Law No. 132/2025 - AI Law (Italy), in the version published on 23 September 2025 (Official Gazette No. 223) entered into force 10 October 2025.

<sup>36</sup> Art. 1 and 222-19 of the Legislative Decree (Italy), in the version published on 8 June 2001 (Official Gazette No. 231).

<sup>37</sup> Law No. 132/2025 - AI Law (Italy), *op. cit.*, note 13.

<sup>38</sup> Art. 31 of the Criminal Code (Spain), Official Gazette No. 10/1995.

<sup>39</sup> Art. 350a para. 1 of the Criminal Code (Netherlands), in the version published on 1 April 1881 (Official Gazette No. 35), as last amended of the Act of 19 April 2005 (Official Gazette No. 211).

<sup>40</sup> Art. 3 of the Corporate Liability Act (Austria), Official Gazette I No. 151/2005.

ings. In this way, liability is focused on control mechanisms rather than on the autonomy of the technology itself.

#### 4.4. Comparative Synthesis

Across all analysed systems, a common element is the preservation of the principle of personal guilt. No State recognises AI as a subject of criminal law. Accordingly, the anthropocentric character of criminal law remains an unquestioned doctrinal constant of the European legal space.

Accordingly, criminal liability may extend to: the programmer, the manufacturer, the user, or the responsible person within a legal entity, depending on their specific contribution and breach of duty in the concrete case. From a comparative perspective, the Croatian model goes a step further, as it explicitly criminalises the use of an AI system in hazardous circumstances, thereby normatively recognising the specificity of technological risk.

Such a normative formulation potentially broadens the scope of criminal law intervention even before concrete harm occurs. This distinguishes the Croatian model from more conservative approaches and raises concerns regarding the potential expansion of criminal liability into areas traditionally governed by regulatory or civil law mechanisms. This approach also risks over-criminalisation if not interpreted restrictively.

#### 4.5. EU Multi-Level Framework

At the EU level, the regulatory framework is shaped by the AI Act, which is preventive in nature (*ex ante*), while the civil liability regime has been modernised through the Revised Product Liability Directive. Criminal liability remains a national domain, but must be consistent with the Charter of Fundamental Rights of the European Union. This creates a multi-layered system of liability, in which national criminal law norms are integrated into the broader European regulatory context.

In this respect, three liability regimes function complementarily: administrative fines (regulatory level), compensation for damage (civil law level), and imprisonment or pecuniary sanctions (criminal law level). The overlap of these regimes requires careful interpretation to avoid double punishment (*ne bis in idem*). The boundaries between these regimes become particularly sensitive in cases involving high-risk AI systems.

National criminal law norms must be proportionate, precise, and foreseeable. The principle of legality (*nullum crimen sine lege*) requires a clear and determinate defi-

nition of prohibited conduct, particularly in technologically complex areas such as AI. Criminal law intervention must be justified by a real and serious risk to protected legal interests (life, bodily integrity, or property of significant value). Otherwise, there would be a risk of overly broad interpretation and potential undermining of legal certainty.

Different national models may give rise to varying standards of criminal liability, regulatory forum shopping, understood as the possibility for economic actors to structure their activities in jurisdictions with more favourable liability standards, and legal uncertainty for multinational technology companies. In this context, the CJEU may play an important role, as its interpretation of the principles of proportionality, legal certainty, and *ne bis in idem* could indirectly influence the shaping of criminal law standards in the field of AI. Case law at the EU level may thus act as a factor of gradual harmonisation without the formal unification of criminal law.

#### **4.6. Key Challenges**

Such a comparative analysis shows that the Croatian reform represents a normatively bold, yet doctrinally sensitive, step forward. Most EU Member States continue to rely on general criminal law doctrines and established models of liability for legal persons.

Key challenges, however, remain: the precise attribution of responsibility within complex technological chains; establishing causation in self-learning systems; distinguishing negligence from permissible technological risk; preserving the principle of personal guilt; and preventing disguised objective liability. Addressing these challenges requires an interdisciplinary approach, particularly the integration of legal and technical expertise.

#### **4.7. Doctrinal implications**

It may be said that the European legal space is currently in a phase of experimental normative adaptation. Future development will likely move towards a gradual convergence of standards, but without a complete unification of criminal law, which remains strongly anchored in national legal traditions.

In this way, AI becomes a test of the resilience of fundamental criminal law principles: personal guilt, proportionality, legality, and subsidiarity. The preservation of these principles in the digital age will determine the long-term legitimacy of criminal law intervention in the field of AI.

The regulation of AI in criminal law raises fundamental questions concerning conduct, causation, and guilt in technologically complex environments. In other words, it is a challenge that affects the very doctrinal structure of criminal law, rather than merely its application to new technological phenomena.

Traditional criminal law theory proceeds from the presumption of conscious and volitional human action as the fundamental unit of criminal law analysis, in which human awareness and control over behaviour constitute a key element in the attribution of guilt. Autonomous systems, however, introduce complex, statistically conditioned decision-making processes that are not always transparent or predictable, relying on probabilistic models and the processing of large volumes of data. For this reason, the establishment of effective supervision is of indisputable importance.

This is particularly evident in the case of machine learning systems, which over time modify their behavioural patterns based on new data, thereby diverging further from their initial programming. In such situations, the question arises whether the classical standard of foreseeability of harmful consequences can be applied without adjustment, or whether more nuanced criteria for assessing negligence must be developed that take into account the technological complexity and dynamism of the system.

This also raises the question of whether the boundaries of permissible risk should be redefined in the context of experimental and innovative technologies. In particular, it invites reconsideration of how foreseeability should be assessed in environments characterised by probabilistic and data-driven decision-making.

The limited transparency of complex AI systems may complicate the assessment of subjective elements of criminal liability. This problem is not merely technical, but has direct implications for establishing the subjective elements of a criminal offence.

This increases the importance of documentation, testing, and transparency as indirect indicators of due care. In the future, procedural rules of evidence may become as important as substantive norms, given that the success of criminal prosecution will largely depend on the ability to reconstruct technical processes and decision-making within algorithmic systems.<sup>41</sup>

#### **4.8. Final Synthesis**

From a comparative perspective, it can be observed that EU Member States balance differently between the promotion of innovation and repressive intervention,

---

<sup>41</sup> Novokmet, A.; Roksandić, S.; Vidaković I., *op. cit.*, note 37.

depending on their respective legal traditions and regulatory philosophies. States that rely more heavily on existing criminal law doctrines implicitly prioritise stability and legal certainty, considering that the technological neutrality of norms allows their application to new forms of risk without the need for specific incriminations.

On the other hand, the Croatian model demonstrates a greater willingness to normatively anticipate risks and to explicitly recognise AI as a source of specific hazards. Such anticipatory criminalisation has a preventive potential, as it sends a clear signal regarding the boundaries of permissible conduct, but it simultaneously carries the risk of overreaching into the domain of permissible technological experimentation and innovation.

The boundary between justified risk and criminally relevant negligence thus becomes extremely sensitive, and its delineation requires careful evaluation of social benefit and potential harm. The attribution of liability remains particularly complex in multi-layered technological chains involving developers, data providers, system integrators, and end users, each exercising different levels of control and knowledge.

The criminal law system, which traditionally requires a clearly identifiable person and precisely established subjective liability, must adapt to the analysis of collective and organisational failures without abandoning the fundamental principles of personal responsibility. It is precisely here that the concept of organisational negligence comes into play, developing through the practice of liability of legal persons and enabling the sanctioning of structural weaknesses in risk management. In this way, the focus shifts from individual error to systemic deficiencies in supervision, control, and corporate security.

At the European level, an additional dimension is the need to align criminal law standards with fundamental rights, in particular the right to a fair trial and the principle of proportionality, which act as a corrective on any repressive intervention. Any criminal norm relating to AI must be formulated with sufficient precision so that its addressees can foresee which conduct is prohibited and what consequences may follow in the event of a violation. Otherwise, there would be a breach of the principle of legality and legal certainty, potentially giving rise to constitutional and European law challenges.

Technological complexity must not serve as an excuse for normative indeterminacy, as this would undermine the legitimising basis of criminal law. Clarity and foreseeability of norms form the foundation of trust in the criminal justice system.

In the long term, it can be expected that specific standards of due care in the AI sector will gradually emerge, developing through case law and regulatory guid-

ance. In fields such as traffic or medical law, where specific standards of professional diligence have evolved, comparable criteria may develop in the AI domain that take into account the level of system autonomy, the foreseeability of risks, the quality of training data, and the availability of safety measures.

These standards would not necessarily require a new category of guilt, but would clarify the content of the existing concept of negligence in the digital context and enable a more consistent application of the law. In this way, they would ensure a balance between flexibility and legal certainty.

The regulation of AI in criminal law reflects the broader challenge of adapting legal systems to technological change while preserving fundamental principles. Criminal law, as the strictest form of social control, must intervene cautiously and subsidiarily, bearing in mind that punishment is a measure of last resort for the protection of fundamental values.

At the same time, criminal law must address serious risks to life, bodily integrity, and property, particularly where they result from systemic failures or breaches of safety standards. This requires a careful balance between innovation and the protection of fundamental values. It is within this balance that it will be determined whether the criminal law systems of EU Member States can preserve their anthropocentric structure while effectively responding to the challenges of autonomous technologies and ensuring the long-term legitimacy of criminal law intervention in the digital age.

## 5. CONCLUSION

An analysis of the European and Croatian normative frameworks shows that legal regulation of AI is developing along two complementary, yet still insufficiently integrated, trajectories. At the EU level, the adoption of the AI Act established a sophisticated preventive, risk-based regulatory model. This model is primarily aimed at ex ante risk management, transparency, conformity assessment, and administrative supervision. In parallel, the reform of liability for defective products through the Revised Product Liability Directive<sup>42</sup> expanded the concept of “product” to include software and AI systems, thereby adapting the civil liability framework to the digital environment.

---

<sup>42</sup> Directive (EU) 2024/2853, *op. cit.*, note 17. Entered into force on 9 December 2024, replacing the nearly 40-year-old regulation from 1985. EU Member States have until 9 December 2026 to transpose it into their national legislation.

This has created a multi-layered system where administrative and market regulation are strongly harmonised, while criminal liability remains fragmented. Such asymmetry generates risks to legal certainty, particularly in cross-border situations and involving multinational technology actors.

This asymmetry is a structural consequence of the constitutional allocation of competences within the European Union, under which criminal law remains primarily within the jurisdiction of Member States. It should therefore not be understood as a regulatory deficiency, but as an inherent feature of the EU legal order.

The Croatian reform of the Criminal Code in 2025 represents a significant step, as it explicitly criminalises the endangerment of life and property through the use of AI systems for the first time. By introducing a statutory definition of an AI system, drawn from the European regulatory framework, formal alignment with EU law has been ensured. At the same time, the new criminal offence is placed among offences against public safety (Chapter XXI of the Criminal Code/11), thereby normatively recognising AI as a specific source of technological risk.

At the same time, it must be emphasised that the primary responsibility for defining the scope and limits of criminal liability lies with the legislator. Without sufficiently precise legislative guidance, there is a risk that courts may be required to resolve fundamental normative questions through interpretation, potentially undermining the principle of legality. Courts play a crucial role in interpreting and applying criminal law norms, but the determination of offences and sanctions must be clearly established through legislation in accordance with the principles of legality and proportionality.

The key findings of this study are as follows. First, the European regulatory model, based on prevention and risk management, does not fully resolve the question of *ex post* liability, particularly in the criminal law context. Second, the Croatian legislator has sought to fill this gap through anticipatory criminalisation, but such an approach requires extremely restrictive and precise interpretation in order to preserve the principles of legality and personal guilt. Third, comparative analysis shows that most Member States continue to apply general criminal law doctrines without specific AI-related incriminations, relying on the individualisation of guilt of programmers, manufacturers, operators, or responsible persons within legal entities.

In all the models analysed, the anthropocentric structure of criminal law is preserved: AI cannot be a bearer of criminal liability. Normative attribution remains attached to a human being or a legal person, while the AI system is regarded as an instrument, a source of risk, or a technical intermediary. In this way, the continu-

ity of fundamental criminal law principles is maintained despite the technological transformation of society.

A particular challenge identified in this paper concerns establishing causation and the subjective element of guilt in the context of complex, self-learning, and partially opaque systems. The “black box” problem, the dynamic adaptability of models, and multi-layered technological chains complicate the precise individualisation of responsibility. In this regard, procedural issues (standards of evidence, expert assessments, access to technical documentation) become as important as the substantive construction of the criminal offence.

Firstly, it shows that the question of liability for AI is not merely technical or regulatory, but raises fundamental questions concerning the concepts of criminal law: conduct, causation, guilt (intent and negligence), and permissible risk. AI tests the resilience of the classical theory of conscious and volitional human action, as it introduces statistically conditioned and autonomous decision-making processes that are not always fully predictable or controllable.

Secondly, the study confirms that it is not necessary to abandon existing criminal law categories in order to address the challenges posed by AI. This conclusion follows from the comparative analysis, which demonstrates that multiple legal systems successfully address AI-related risks through the application of general doctrines of negligence and organisational fault, without introducing fundamentally new categories of criminal liability.

Rather than creating a “new” type of guilt or attributing legal personality to algorithms, it is possible to adapt existing doctrines, particularly negligence and organisational fault, to the technological context. In this way, the continuity of legal tradition is maintained, and normative radicalism that could destabilise the criminal law system is avoided.

Thirdly, the analysis of the Croatian reform highlights both the advantages and risks of anticipatory criminalisation. The advantage lies in the fact that the use of AI systems in hazardous circumstances is subject to criminal law control. This strengthens the preventive function of the law and public confidence in the safe application of new technologies. The risk, however, lies in the potential for overly broad interpretation and disguised objective liability, particularly if standards of due care are not defined with precision.

Fourthly, the study emphasises the need for a clear distinction between criminal and civil liability. The civil law regime has a primarily reparative function, whereas criminal law protects fundamental social values and operates as *ultima ratio*. Any

erosion of this distinction would lead to an approximation to objective liability, which would be contrary to the principles of proportionality and personal guilt guaranteed within the European legal space.

Fifthly, the comparative overview shows that EU Member States are currently in a phase of normative experimentation. The Croatian model represents one of the first attempts at explicit AI-related incrimination, whereas other states prefer a technologically neutral approach.

This diversity can serve as an impetus for the development of best practices, but it simultaneously creates a risk of fragmentation and regulatory “forum shopping.” This may occur where economic actors choose to develop, deploy, or structure AI-related activities in jurisdictions with less stringent standards of criminal liability, thereby potentially undermining the uniform level of protection across the internal market.

In this way, the study supports the thesis that the future development of criminal liability for AI will not move toward complete unification, but rather toward a gradual convergence of standards through case law, doctrine, and mutual learning between legal systems. Based on the analysis conducted, several guidelines can be formulated for the further development of criminal law regulation of AI, both at the national and European levels. Any criminal norm relating to AI must be formulated clearly and predictably. Definitions drawn from regulatory law must be interpreted restrictively in the criminal law context, with the consistent application of the principle *in dubio pro reo*.

In complex technological chains, it is essential to precisely establish the personal contribution of an individual or organisational failure within a legal person. Criminal liability must not be based solely on the fact that an AI system caused harm, but rather on a demonstrable failure in its design, supervision, or use.

In practice, these criteria will need to be concretised through case law, particularly with regard to the level of system autonomy, the foreseeability of risks, the quality of training data, and the availability of safety mechanisms. In this way, the content of negligence in the digital context would be clarified.

The effective application of criminal law in this field depends on the development of specialised expert evidence, as well as on the capacity of courts to assess complex technical processes, particularly in cross-border cases. This includes, in particular, the development of forensic methodologies for analysing algorithmic decision-making, access to technical documentation and training data, and the establishment of interdisciplinary expert bodies capable of bridging legal and tech-

nical knowledge. Without adequate evidentiary tools, the criminal law norm will remain purely declaratory.

Administrative sanctions, civil compensation, and criminal liability must be coordinated to avoid double punishment and the violation of the principle of *ne bis in idem*. A clear hierarchy of interventions will strengthen legal certainty.

Criminal law intervention must remain reserved for serious and concrete violations of fundamental interests - life, bodily integrity, and property of significant value. Innovative technological development must not be unjustifiably constrained by fear of criminal sanctions, but neither should it be exempt from liability in cases of conscious or gross disregard of safety standards.

Ultimately, AI does not require the abandonment of the fundamental principles of criminal law, but rather their careful and thoughtful adaptation to new circumstances. The future of criminal law regulation of AI will depend on the ability of the legal system to preserve its normative core while responding to technological complexity.

It is in this balance between continuity and adaptation that the long-term legitimacy of criminal law intervention in the digital age lies. The legitimacy of criminal law in the age of artificial intelligence will depend not on its expansion, but on its ability to adapt without abandoning its fundamental principles. Only such a balanced approach can ensure both effective protection of fundamental values and the preservation of legal certainty in an increasingly autonomous technological environment.

## REFERENCES

### BOOKS AND ARTICLES

1. Berdica, J.; Herceg Pakšić, B., *Umjetna inteligencija i odabrani aspekti kaznenoga prava. O nekim izazovima za suvremenu pravnu kulturu*, Filozofska istraživanja, Vol. 42, Issue 1, 2022, pp. 87-102
2. Cartier M. E., *Kaznenopravna odgovornost pravnih osoba u francuskom pravu*, Hrvatski ljetopis za kazneno pravo i praksu, Vol. 12, Issue 2, 2005, pp. 279-293
3. Dragičević Prtenjača, M.; Roksandić, S., *Criminal Law and Criminal Compliance in Croatia*, in: Papathanasiou, K. (ed.), *Corporate Criminal Law and Criminal Compliance*, Vienna, 2023, pp. 137-164
4. Ebers, M. et al., *The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS)*, J, Vol. 4, Issue 4, 2021, pp. 589-603

5. Gless, S.; Silverman, E.; Weigend, T., *If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability*, New Criminal Law Review, Vol. 19, Issue 3, 2016, pp. 412-436
6. Marchant, G. E.; Lindor, R. A., *The Coming Collision Between Autonomous Vehicles and the Liability System*, Santa Clara Law Review, Vol. 52, Issue 4, 2012, pp. 1321-1340
7. Moch, E., *Autonomous Systems (AI) and Criminal Imputability: Challenges for Modern Law*, International Journal of Research and Review, Vol. 12, Issue 10, 2025, pp. 287-301
8. Mrčela, M.; Vuletić, I., *Novo kazneno djelo – dovođenje u opasnost života i imovine sustavom umjetne inteligencije*, Državno odvjetništvo otvara razgovor: DOOR, Vol. 1, Issue 1, 2025, pp. 219-231
9. Novelli, C. et al., *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*, Computer Law & Security Review, Vol. 55, 106066, 2024
10. Novokmet, A.; Roksandić, S.; Vidaković I., *Tehnološki potaknute promjene u kaznenom postupku: održavanje ravnoteže učinkovitosti kaznenog postupka i prava na obranu*, in: Modernizacija prava, Knjiga 82., Regulacija umjetne inteligencije u Europskoj uniji: Tehnološki izazovi i etička pitanja, pp. 63-98
11. Novoselec, P. (ed.), *Posebni dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2007
12. Rodríguez de Las Heras Ballel, T., *Mapping Generative AI rules and liability scenarios in the AI Act, and in the proposed EU liability rules for AI liability*, Cambridge Forum on AI: Law and Governance, Vol. 1, Issue e5, 2025, pp. 1-23
13. Roksandić, S.; Engelhart, M., *Environmental Corruption: Fighting Two Evils through International Criminal Law Alongside Introducing a Special Protocol to UNCAC and UNTOC*, International Criminal Law Review, Vol. 25, Issue 2-3, 2025, pp. 247-270
14. Roksandić, S.; Protrka, N.; Engelhart, M., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?*, in *Proceedings of the 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, IEEE, 2022
15. Roksandić Vidlička, S.; Liepiņa, E.; Ostapchuk, S., *Bioethical and Legal Challenges of Artificial Intelligence and Human Dignity*, in: Jovanović, M.; Virady, Tibor (eds.), *Human Rights in 21st Century*, Netherlands, 2020, pp. 269-288
16. Tran, H. C., *Unbounded Harms, Bounded Law: Liability in the Age of Borderless AI*, J, arXiv preprint arXiv:2601.12646, 2026
17. Vuletić, I.; Novokmet, A.; Tomičić, Z., *Izazovi posebnog dijela kaznenog prava zbog razvoja umjetne inteligencije uz poseban osvrt na hrvatsko kazneno pravo*, Zbornik Pravnog fakulteta u Zagrebu, Vol. 47, Issue 1, 2024, pp. 5-33
18. Wagner, G., *Liability Rules for the Digital Age – Aiming for the Brussels Effect*, Journal of European Tort Law, Vol. 13, Issue 3, 2023, pp. 191-243

## COURT OF JUSTICE OF THE EUROPEAN UNION

1. Case C-131/12 Google Spain SL and Mario Costeja González [2014] 2012/C 165/18
2. Case C-492/23 – Russmedia Digital SRL and Inform Media Press SRL [2025] ECLI:EU: C:2025:935

## EUROPEAN COURT OF HUMAN RIGHTS

1. *Cantoni v France* (1996) 35 ECHR 121
2. *Kokkinakis v Greece* (1993) 52 ECHR 20

## EU LAW AND REGULATION

1. Charter of Fundamental Rights of the European Union [2012] OJ C 326/391
2. High Level Expert Group on Artificial intelligence set up by the European Commission, *Ethics Guidelines for Trustworthy AI*, 2019, Available at: [<https://www.aepd.es/sites/default/files/2019-12/aiethics-guidelines.pdf>], Accessed 26 March 2026
3. Directive (EU) 2024/1203 of the European Parliament and of the Council of 11 April 2024 on the protection of the environment through criminal law and replacing Directives 2008/99/EC and 2009/123/EC [2024] OJ L, 2024/1203
4. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC [2024] OJ L, 2024/2853 (Text with EEA relevance)
5. Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, E.T.S. No. 5, 213 U.N.T.S. 222
6. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] OJ L2024/1689 (Artificial Intelligence Act) (Text with EEA relevance)

## LIST OF NATIONAL REGULATIONS, ACTS AND COURT DECISIONS

1. Law on the Liability of Legal Persons for Criminal Offences (Croatia), Official Gazette No. 151/03, 110/07, 45/11, 143/12, 114/22, 114/23
2. Corporate Liability Act (Austria), Official Gazette I No. 151/2005
3. Criminal Code (Croatia), Official Gazette No. 144/2012, 125/2011, 56/2015, 61/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022, 114/2023, 36/2024, 136/2025
4. Criminal Code (France), in the version published on 29 July 1994 (Official Gazette No. 175), as last amended of the Act of 9 July 2025 (Official Gazette No. 622)
5. Criminal Code (Germany), in the version published on 13 November 1998 (Official Gazette I, p. 3322), as last amended by Article 2 (2) of the Act of 7 November 2024 (Official Gazette 2024 I No. 351)
6. Criminal Code (Netherlands), in the version published on 1 April 1881 (Official Gazette No. 35), as last amended of the Act of 19 April 2005 (Official Gazette No. 211)
7. Criminal Code (Spain), Official Gazette No. 10/1995
8. Judgement of the Supreme Court of the Republic of Croatia No. I Kž 438/2018-11 of 21 October 2020

9. Judgement of the Supreme Court of the Republic of Croatia No. I Kž 561/2020-9 of 15 April 2021
10. Law No. 132/2025 - AI Law (Italy), in the version published on 23 September 2025 (Official Gazette No. 223)
11. Legislative Decree (Italy), in the version published on 8 June 2001 (Official Gazette No. 231)

## WEBSITE REFERENCES

1. Euronews, *EU Tech Commissioner defends scrapping of AI Liability rules*, 2025, Available at: [https://arxiv.org/html/2503.05787v2], Accessed 12 January 2026
2. European Commission, *On the road to automated mobility: An EU strategy for mobility of the future* COM(2018) 283 final, Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0283], Accessed 26 March 2026
3. European Parliament, *Artificial Intelligence Liability Directive*, 2025, Available at: [https://arxiv.org/html/2503.05787v2], Accessed 11 January 2026
4. Kritikos, M., *Artificial Intelligence ante portas: Legal & ethical reflections*, 2019, Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/634427/EPRS\_BRI(2019)634427\_EN.pdf], Accessed 26 March 2026
5. Lewis, D; Lasek-Markey M.; Golpayegani D.; J Pandit, H., *Mapping the Regulatory Learning Space for the EU AI Act*, 2025, Available at: [https://arxiv.org/html/2503.05787v2], Accessed 10 January 2026