Tadqiqot uz

ISSN 2181-9130

Doi Journal 10.26739/2181-9130

ҲУҚУҚИЙ ТАДҚИҚОТЛАР ЖУРНАЛИ

11 ЖИЛД, 5 СОН

ЖУРНАЛ ПРАВОВЫХ ИССЛЕДОВАНИЙ

ТОМ 11, НОМЕР 5

JOURNAL OF LAW RESEARCH

VOLUME 11, ISSUE 5

ТОШКЕНТ-2026

ҲУҚУҚИЙ ТАДҚИҚОТЛАР ЖУРНАЛИ

ЖУРНАЛ ПРАВОВЫХ ИССЛЕДОВАНИЙ | JOURNAL OF LAW RESEARCH

№5 (2026) DOI http://dx.doi.org/10.26739/2181-9130-2026-5

Контакт редакций журналов. www.tadqiqot.uz
ООО Tadqiqot город Ташкент,
улица Амира Темура пр.1, дом-2.
Web: http://www.tadqiqot.uz/; Email: info@tadqiqot.uz
Тел: (+998-94) 404-0000

Editorial staff of the journals of www.tadqiqot.uz
Tadqiqot LLC the city of Tashkent,
Amir Temur Street pr.1, House 2.
Web: http://www.tadqiqot.uz/; Email: info@tadqiqot.uz
Phone: (+998-94) 404-0000

МУНДАРИЖА | СОДЕРЖАНИЕ | CONTENT

ISSN: 2181-9130
www.tadqiqot.uz
ҲУҚУҚИЙ ТАДҚИҚОТЛАР ЖУРНАЛИ
ЖУРНАЛ ПРАВОВЫХ ИССЛЕДОВАНИЙ | JOURNAL OF LAW RESEARCH

12.00.08-УГОЛОВНОЕ ПРАВО. УГОЛОВНО-ИСПОЛНИТЕЛЬНОЕ ПРАВО

Khamidov Nurmukhammad Orif ugli,
Acting Professor of the Department of Criminal Law, Criminology
and Anti-Corruption of Tashkent State University of Law,
Doctor of Philosophy (PhD) in Law
E-mail: hamidov-2018@list.ru
Najimova Jamola Davron qizi,
2nd year student of the Faculty of Criminal Justice
at Tashkent State University of Law
E-mail: najimovajamola@gmail.com

ARTIFICIAL INTELLIGENCE AND THE FUTURE OF CRIMINAL LIABILITY: A COMPARATIVE LEGAL ANALYSIS

For citation: Khamidov Nurmukhammad Orif ugli, Najimova Jamola Davron qizi. ARTIFICIAL INTELLIGENCE AND THE FUTURE OF CRIMINAL LIABILITY: A COMPARATIVE LEGAL ANALYSIS. Journal of Law Research. 2026, 11 vol., issue 5.

http://dx.doi.org/10.5281/zenodo.22235163

ANNOTATION

This article examines the criminal liability challenges arising from the rapid advancement of artificial intelligence (AI) technologies. It analyses the theoretical foundations of liability attribution for offences committed by or through AI systems, with particular focus on the application of the mens rea and actus reus doctrines in the AI context. A comparative analysis is conducted across the legal systems of the United States, the European Union, China, Germany, and other leading jurisdictions. The article also addresses contemporary issues including deepfake fraud, lethal autonomous weapon systems, and AI-driven financial crime. The study concludes that existing legislative frameworks are inadequate and argues for targeted legal reforms, including dedicated AI criminal liability norms, strict liability standards, and enhanced international cooperation.

Keywords: artificial intelligence, criminal liability, mens rea, actus reus, comparative law, AI legislation, autonomous systems, EU AI Act, responsibility gap, digital criminal law.

Hamidov Nurmuhammad Orif o‘g‘li,
Toshkent davlat yuridik universiteti
Jinoyat huquqi, kriminologiya va korrupsiyaga qarshi
kurashish sho‘basi professori vazifasini bajaruvchisi,
Yuridik fanlar bo‘yicha falsafa doktori (PhD)
E-mail: hamidov-2018@list.ru
Najimova Jamola Davron qizi,
Toshkent davlat yuridik universiteti
Jinoiy odil sudlov fakulteti 2-kurs talabasi

E-mail: najimovajamola@gmail.com

SUN’IY INTELLEKT VA JINOIY JAVOBGARLIKNING KELAJAGI: QIYOSIY HUQUQIY TAHLIL

ANNOTATSIYA

Ushbu maqola sun’iy intellekt (SI) texnologiyalarining jadal rivojlanishi munosabati bilan yuzaga kelayotgan jinoiy javobgarlik muammolarini o‘rganishga bag‘ishlangan. Maqolada SI tizimlari tomonidan yoki SI vositasida sodir etilgan huquqbuzarliklarda javobgarlikni belgilashning nazariy asoslari tahlil qilinadi, xususan “mens rea” va “actus reus” doktrinalarining SI kontekstida qo‘llanilishiga alohida e’tibor qaratiladi. Amerika Qo‘shma Shtatlari, Yevropa Ittifoqi, Xitoy, Germaniya va boshqa yetakchi yurisdiktsiyalarning huquqiy tizimlari bo‘yicha qiyosiy tahlil o‘tkaziladi. Maqolada shuningdek “deepfake” texnologiyasi yordamida amalga oshiriladigan firibgarlik, halokatli avtonom qurol tizimlari va SI yordamidagi moliyaviy jinoyatlar kabi dolzarb muammolar ham ko‘rib chiqiladi. Tadqiqot natijasida amaldagi qonunchilik mexanizmlari yetarli emasligi to‘g‘risida xulosa chiqariladi va maqsadli huquqiy islohatlarga, jumladan SI sohasida jinoiy javobgarlikka oid maxsus normalar qabul qilishga, qat’iy javobgarlik standartlarini joriy etishga hamda xalqaro hamkorlikni kuchaytirishga ehtiyoj asoslab beriladi.

Kalit so‘zlar: sun’iy intellekt, jinoiy javobgarlik, mens rea, actus reus, qiyosiy huquq, SI qonunchiligi, avtonomli tizimlar, YeI AI Act, javobgarlik bo‘shlig‘i, raqamli jinoiy huquq.

Хамидов Нурмухаммад Ориф угли,
Исполняющий обязанности профессора кафедры уголовного права, криминологии и противодействия коррупции Ташкентского государственного юридического университета,
Доктор философии по юридическим наукам (PhD)
E-mail: hamidov-2018@list.ru
Нажимова Жамола Даврон кизи,
Студент 2-го курса факультета уголовного правосудия Ташкентского государственного юридического университета
E-mail: najimovajamola@gmail.com

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И БУДУЩЕЕ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ

АННОТАЦИЯ

Настоящая статья посвящена проблемам уголовной ответственности, возникающим в связи с ускоренным развитием технологий искусственного интеллекта (ИИ). В ней анализируются теоретические основы установления ответственности за правонарушения, совершённые с помощью систем ИИ или с их использованием, с особым акцентом на применение доктрин mens rea и actus reus в контексте ИИ. Проводится сравнительный анализ правовых систем Соединённых Штатов Америки, Европейского Союза, Китая, Германии и других ведущих юрисдикций. В статье также рассматриваются актуальные проблемы, включая мошенничество с применением технологии «дипфейк», летальные автономные системы вооружения и финансовые преступления, совершаемые с использованием ИИ. По итогам исследования делается вывод о недостаточности действующих законодательных механизмов и обосновывается необходимость целенаправленных правовых реформ, в том числе принятия специальных норм об уголовной ответственности в сфере ИИ, введения стандартов строгой ответственности и расширения международного сотрудничества.

Ключевые слова: искусственный интеллект, уголовная ответственность, mens rea, actus reus, сравнительное право, законодательство об ИИ, автономные системы, Акт ЕС об ИИ, пробел ответственности, цифровое уголовное право.

I. INTRODUCTION

The rapid integration of artificial intelligence into virtually every domain of modern life — from healthcare diagnostics and financial trading to autonomous vehicles and military systems — presents unprecedented challenges for legal scholars and policymakers alike. While AI brings enormous benefits to society, it also introduces entirely new categories of legal risk. When an AI system causes harm, injures a person, commits fraud, or makes a lethal decision without human input, the question of who bears criminal responsibility becomes deeply complex and, under existing law, often unanswerable.

Classical criminal law is premised on the existence of a human agent capable of forming intent and executing a voluntary act. These two pillars — mens rea (the mental element, or guilty mind) and actus reus (the physical element, or guilty act) — have anchored criminal liability across virtually all legal systems for centuries [1]. Yet autonomous and machine-learning-powered AI systems may act in ways that are entirely unpredictable, even to their own creators. The AI system does not possess consciousness, emotions, or a will. It cannot be imprisoned, fined in a personally meaningful sense, or reformed. The traditional architecture of criminal law thus confronts a category of actor it was never designed to handle.

This article addresses the problem through a comparative legal lens. It surveys how leading jurisdictions — the United States, the European Union, China, and Germany — are currently grappling with AI-related criminal liability, examines the foundational doctrinal tensions that AI creates, and evaluates proposals for legal reform. The analysis draws on recent legislative developments, including the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), which entered into force on 1 August 2024 and represents the world's first comprehensive statutory framework for AI governance [8].

II. THEORETICAL FOUNDATIONS OF CRIMINAL LIABILITY IN THE AI CONTEXT

In both common law and civil law traditions, criminal liability rests on two concurrent elements. Actus reus denotes a prohibited act or omission — the external, physical dimension of the offence. Mens rea denotes the mental state accompanying that act — whether the defendant acted with purpose, knowledge, recklessness, or negligence [1]. The simultaneous presence of both elements constitutes the criminal offence; absent either, liability ordinarily cannot attach.

In common law jurisdictions such as the United States and the United Kingdom, mens rea is typically analysed along a hierarchy of mental states drawn from the Model Penal Code: purpose (the actor consciously desires the result), knowledge (the actor is practically certain the result will follow), recklessness (the actor consciously disregards a substantial and unjustifiable risk), and negligence (the actor fails to perceive a risk a reasonable person would have recognised) [2]. Civil law systems articulate analogous concepts: in German criminal law, the Strafgesetzbuch (StGB) requires proof of Vorsatz (intent) or, where the statute permits, Fahrlässigkeit (negligence), with culpability treated as an indispensable condition of liability [3].

These foundational concepts were developed with human actors in mind. An AI system, however sophisticated, does not form intentions in any legally cognisable sense. It does not deliberate, experience emotion, or act voluntarily. This mismatch is not merely theoretical: it produces concrete gaps in the law every time an AI-driven decision causes harm without a clearly identifiable human decision-maker behind it.

The concept of the 'responsibility gap' — introduced by the German philosopher Andreas Matthias — describes the situation that arises when a machine-learning system departs from its original programming and causes harm in ways that neither its developers nor its operators could have foreseen or prevented [4]. As AI systems become more autonomous, the causal and normative connection between human decisions and AI outcomes grows attenuated. The developer may have exercised reasonable care in designing the system; the operator may have deployed it appropriately; the end user may have done nothing wrong — yet serious harm results.

The responsibility gap is not hypothetical. Research published in 2024-2025 documented more than 800 AI-related harmful incidents where identifying a culpable human actor proved difficult

under existing legal frameworks [5]. In the financial sector, algorithmic trading systems have triggered market disruptions — most notably the 2010 'Flash Crash,' in which automated trading contributed to a dramatic and sudden market collapse — where attributing deliberate wrongdoing was effectively impossible under then-current law [4].

The gap is widened further by the 'black box' problem: many modern deep-learning systems cannot explain their own outputs in human-intelligible terms. If neither the system's designers nor its operators can reconstruct the chain of reasoning that led to a harmful outcome, proving any form of culpable mental state becomes a near-insurmountable evidentiary challenge.

III. COMPARATIVE LEGAL ANALYSIS: MAJOR JURISDICTIONS

The United States currently lacks a federal statute specifically addressing criminal liability for AI-caused harm. Prosecutors and regulators instead apply existing doctrines — wire fraud (18 U.S.C. §1343), the Computer Fraud and Abuse Act (18 U.S.C. §1030), identity theft statutes, and various state-level provisions — to conduct in which AI features as an instrument or enabling technology [6].

The common law doctrine of proximate causation provides a potential vehicle for holding developers, operators, or deployers liable when an AI system causes foreseeable harm. Under the 'sophisticated tool' analogy, the AI system is treated as an inert instrument — like a weapon or a vehicle — and liability is assigned to the human who set it in motion with the relevant mental state. Abbott and Sarch have argued for formalising this approach through a 'legal fiction of criminal liability,' under which AI developers or deployers would be deemed to possess the requisite mens rea where they knowingly created systems capable of harmful autonomous action and failed to implement adequate safeguards [6]. An emerging area of concern in the United States is the use of generative AI in deepfake-based fraud and non-consensual intimate imagery. While some states have enacted specific deepfake statutes, federal coverage remains fragmented, and the rapid pace of AI development consistently outstrips legislative response.

The EU AI Act (Regulation (EU) 2024/1689), formally adopted by the European Parliament on 13 June 2024 and in force since 1 August 2024, is the world's first comprehensive statutory framework for AI [8]. The Act classifies AI systems according to their risk profile: prohibited uses (those posing unacceptable risks, such as social scoring by governments or real-time biometric surveillance in public spaces); high-risk systems (those deployed in critical infrastructure, justice, employment, and education); limited-risk systems; and minimal-risk systems. Significantly, the AI Act does not directly create criminal offences. It establishes obligations — risk assessment, technical documentation, human oversight mechanisms, conformity assessment — whose violation may constitute the predicate for criminal or administrative liability under national law [9]. Several EU member states are already adapting their criminal codes to treat systematic non-compliance with the AI Act's high-risk system requirements as a basis for criminal negligence prosecutions.

The Council of Europe's Committee on Criminal Law (CDPC) published a discussion paper in November 2024 outlining a framework for member states to adapt their criminal law to address AI-related liability [9]. The paper recommends, inter alia, adapting the novus actus interveniens doctrine to AI contexts — so that unforeseen AI behaviour does not automatically break the causal chain leading back to the developer — and developing a concept of 'relevant contributory liability' to address cases where the victim's own conduct (for example, failure to apply required software updates) contributed to the harmful outcome. The CDPC was tasked with producing a binding legal instrument by end-2025.

The EU AI Liability Directive, which would have complemented the AI Act by granting plaintiffs access to AI documentation for civil liability purposes, was proposed in 2022 but ultimately withdrawn in 2025 [9]. This development makes the criminal law track all the more important for effective redress.

Chinese law does not recognise AI systems as legal persons capable of bearing criminal responsibility. Under the current framework, an individual who uses AI as a tool to commit a crime is personally liable under the applicable provisions of the Criminal Law of the People's Republic of China [11]. The AI system is characterised as an instrument, and its use in crime is treated as an aggravating circumstance rather than as raising distinct questions of legal personality.

In September 2023, the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security jointly issued Guiding Opinions on Punishing Cyber Violence and Illegal Crimes in Accordance with the Law. The document explicitly classifies the use of 'deep synthesis' (deepfake) generative AI to produce and disseminate illegal content as a cyber-violence offence, attracting enhanced sentencing [11]. In December 2024, the Ministry of Public Security released ten illustrative cases of criminal liability arising from AI-assisted cyber fraud, reinforcing the instrument-based approach while signalling a willingness to pursue the human actors behind AI-enabled crimes aggressively. China's AI Safety Governance Framework 1.0, published in September 2024 by the National Technical Committee 260, establishes non-binding best-practice guidance for AI developers and deployers across the full AI lifecycle. While not creating criminal liability directly, the Framework establishes normative expectations against which conduct may be measured in subsequent enforcement proceedings.

The contrast between common law and civil law approaches to AI criminal liability reflects deeper structural differences in how each tradition generates legal norms. Common law systems — exemplified by the United States and the United Kingdom — rely on judicial precedent to extend existing doctrine incrementally to novel fact patterns. This produces a degree of contextual flexibility: courts can tailor the application of fraud, negligence, and causation doctrines to AI cases without waiting for legislative action. The disadvantage is unpredictability: defendants and regulators cannot know in advance how courts will resolve genuinely novel questions, and outcomes may diverge significantly across jurisdictions [5].

Civil law systems, typified by Germany and France, prefer codified rules with clearly defined elements. The German StGB, for example, requires proof of Vorsatz (intent) or statutory negligence under a defined standard; courts do not freely extend liability to new categories of actors. This approach offers legal certainty but demands legislative action to address genuinely new problems. Where the legislature has not yet acted — as is largely the case with AI criminal liability — the civil law judge is less able to fill gaps creatively. The consensus in recent scholarship is that neither approach alone is adequate and that a hybrid model — combining the definitional clarity of civil law codification with the adaptive flexibility of the common law — is needed [5]. Crucially, any effective framework must be sufficiently international in scope: AI systems and the harms they cause traverse jurisdictional boundaries with ease, and a patchwork of inconsistent national rules creates regulatory arbitrage opportunities that sophisticated actors can readily exploit.

IV. ATTRIBUTION OF CRIMINAL LIABILITY: WHO BEARS RESPONSIBILITY?

AI developers occupy the primary position in the chain of causation from system design to harmful outcome. Under product liability principles, a developer may be civilly liable for defects in an AI system regardless of fault. For criminal liability, however, the mens rea requirement demands something more: at a minimum, the developer must have known, or ought to have known, that the system was capable of producing the harmful outcome in question [2].

The EU AI Act imposes extensive ex ante obligations on providers of high-risk AI systems, including conformity assessments, technical documentation, and post-market monitoring. Systematic non-compliance with these obligations — particularly where the developer was aware of the risks — may satisfy the recklessness or gross negligence standard required for criminal liability in many jurisdictions [9]. A developer who deliberately conceals known safety failures from regulators while continuing to deploy a dangerous system would, in most jurisdictions, satisfy even an intent-based standard.

Where an AI system is deployed by an operator (a business or institution) or used by an end-user to commit a crime, the analysis is considerably more straightforward. A user who employs an AI image-generation tool to create deepfake content for purposes of blackmail, defamation, or financial fraud is directly liable for the underlying offence; the AI is simply the instrument of the crime [7]. Professor Gabriel Hallevy's 'Innocent Agent Model,' elaborated in his chapter on criminal liability models for AI systems, provides the most widely cited analytical framework for this scenario [12]. The model treats the AI as an innocent agent — analogous to a person acting without knowledge or consent — while the criminal liability attaches fully to the human who set the system in motion

with the relevant criminal purpose. This model fits comfortably within existing common law and civil law frameworks and currently represents the dominant approach in operational legal systems worldwide.

More difficult questions arise where the operator uses AI in a context where harm is foreseeable but not intended. An operator who deploys a facial-recognition system knowing it has high rates of false positives in a particular demographic group, and who nonetheless relies on its outputs to make arrest decisions, may be criminally negligent even if no specific harmful outcome was desired.

A more radical strand of scholarship argues that sufficiently advanced autonomous AI systems should be granted a form of legal personality — an 'electronic personhood' — that would allow them to bear rights and obligations, including criminal liability, independently of their human principals [14]. Proponents of this view point to the legal personhood already accorded to corporations and argue that the underlying policy justification — enabling coherent legal relations with entities that exercise real-world agency — applies equally to autonomous AI. The counterarguments are, however, formidable. Criminal punishment serves multiple functions: deterrence, incapacitation, rehabilitation, and retribution. An AI system cannot be deterred (it lacks preferences about its own future states), incapacitated in a meaningful sense (it can be switched off, but copies may persist), rehabilitated, or made to suffer the expressive condemnation that criminal conviction embodies [15]. Extending criminal liability to AI entities would risk creating a legal shield behind which human developers and operators could avoid accountability. The European Parliament's 2017 resolution on robotics, which floated the concept of electronic personhood for liability purposes, was ultimately not incorporated into the AI Act, and the EU has since moved away from the idea.

V. CONTEMPORARY CHALLENGES: DEEPFAKES, AUTONOMOUS WEAPONS, AND ALGORITHMIC CRIME

Deepfake technology — the use of generative AI to create synthetic audio-visual content depicting real individuals in fabricated situations — has emerged as one of the fastest-growing vectors for AI-assisted crime. According to data cited in recent comparative research, trading in deepfake tools on dark web forums increased by 223% in 2024, and AI-based fraud losses are projected to reach USD 40 billion globally by 2027 [5]. In the first quarter of 2025, 87% of major organisations worldwide reported having experienced at least one AI-based cyberattack. The criminal law problems posed by deepfakes are substantial. In most jurisdictions, the applicable offences — fraud, defamation, extortion, non-consensual intimate imagery — were not drafted with synthetic media in mind and require adaptation. Key evidentiary questions include: how to authenticate or de-authenticate AI-generated content; whether detection tools are sufficiently reliable to ground a criminal conviction; and how to attribute the creation of deepfake material to a specific defendant when generation tools are widely accessible and leave minimal forensic traces.

Lethal Autonomous Weapon Systems (LAWS) — systems capable of selecting and engaging targets without meaningful human control — represent perhaps the most acute criminal law challenge posed by AI. When a LAWS kills a civilian in violation of international humanitarian law, the question of criminal responsibility is both practically and doctrinally unresolved. The Geneva Conventions and their Additional Protocols, drafted long before the advent of autonomous systems, offer no explicit guidance on the liability of states or individuals where the decision to use force was made by a machine.

International criminal law requires, for individual criminal liability, proof of command responsibility or direct participation. Where an autonomous system executes an unlawful strike, the chain of command connecting the human decision to activate the system and the specific harmful outcome may be attenuated to the point that individual criminal liability cannot be established under existing doctrine. Many legal scholars and states have consequently called for a new international treaty specifically prohibiting LAWS that lack meaningful human control, analogous to the prohibitions on anti-personnel mines and cluster munitions.

Algorithmic trading systems capable of executing millions of transactions per second have been implicated in market manipulation and financial instability. The 2010 Flash Crash — in which

the Dow Jones Industrial Average lost approximately 9% of its value within minutes before partially recovering — illustrated the systemic risks posed by AI-driven financial systems operating without adequate human oversight [4]. Criminal prosecutions for algorithmic market manipulation are technically and legally complex. Prosecutors must prove that the algorithm was designed to produce manipulative outcomes (purpose), or that its deployers knew it would do so (knowledge), or at minimum that its dangerous characteristics were foreseeable (recklessness or negligence). Given the opacity of many algorithmic systems, establishing any of these mental states beyond reasonable doubt is challenging. Some jurisdictions have responded by shifting to strict liability or administrative penalty regimes for certain categories of algorithmic trading misconduct, bypassing the mens rea requirement entirely.

VI. THE CASE FOR REFORM: RECOMMENDATIONS

The foregoing analysis demonstrates that existing criminal law frameworks, in both common law and civil law jurisdictions, are structurally ill-equipped to address the full range of AI-related criminal liability. Four principal reforms are warranted.

First, jurisdictions should enact dedicated AI criminal liability provisions establishing clear, differentiated standards for developers, operators, and users. These provisions should specify the mental states (intent, recklessness, gross negligence) sufficient for liability at each level of the AI supply chain, and should define the circumstances in which vicarious or strict liability is appropriate. The EU AI Act's risk-based classification offers a useful template: liability standards could be calibrated to the risk tier of the system involved.

Second, for high-risk AI applications — autonomous vehicles, medical AI, and public safety systems — strict liability or enhanced negligence standards should apply. Requiring proof of subjective mens rea in these contexts is both doctrinally inconsistent (comparable product liability regimes do not impose such requirements) and practically unworkable (the opacity of AI systems makes subjective intent virtually impossible to establish). Placing the burden of proving adequate risk mitigation on developers and operators creates appropriate incentives for safe design.

Third, international legal cooperation is essential. The Budapest Convention on Cybercrime provides a partial model, but its provisions do not address AI-specific criminal conduct. A dedicated multilateral instrument — potentially a new Protocol to the Budapest Convention or a free-standing AI crime treaty — is needed to facilitate cross-border evidence gathering, harmonise criminal definitions, and prevent regulatory arbitrage. The Council of Europe's CDPC process, if it produces a binding instrument by its 2025 deadline, will be an important step in this direction [9].

Fourth, the Republic of Uzbekistan, like many developing and transition economies, faces the dual challenge of capturing the benefits of AI adoption while building adequate legal safeguards. The Presidential Decree on Artificial Intelligence (2020) and the Digital Development Strategy 2022-2030 provide a framework for AI governance, but the criminal liability dimension has not yet been systematically addressed. Uzbekistan should consider incorporating dedicated AI criminal liability norms into the Criminal Code, drawing on comparative experience from the jurisdictions analysed above, and should engage actively in international norm-setting processes.

VII. CONCLUSION

Artificial intelligence and criminal liability represent one of the defining legal challenges of the twenty-first century. This comparative analysis has demonstrated that the traditional pillars of criminal law — mens rea and actus reus — are ill-suited to the characteristics of autonomous AI systems, which may cause serious harm without any identifiable human mental state driving the specific harmful outcome. The responsibility gap is real, it is growing, and existing law does not close it.

The EU AI Act (2024) is a significant step towards a principled regulatory framework, but it does not directly create criminal offences and leaves the liability question largely to member states. China's instrument-based approach is clear and pragmatic but may struggle to keep pace with more sophisticated AI-enabled harms. The United States continues to rely on doctrinal adaptation by courts and prosecutors, with all the attendant uncertainty. None of these approaches fully solves the problem.

The way forward requires dedicated legislative action at both national and international levels, adopting a hybrid model that combines civil law certainty with common law flexibility, calibrated to the specific risk characteristics of different AI applications. Crucially, the reforms must ensure that human accountability is preserved and strengthened, not diluted, as AI systems become more autonomous. The challenge is not merely technical or doctrinal: it is a question of whether law can maintain its fundamental commitment to justice in the face of technologies that do not fit its foundational categories.

References/Iqtiboslar/Сноски:

1. Horder, J. Ashworth's Principles of Criminal Law. 10th ed. — Oxford: Oxford University Press, 2022. — 608 p. https://doi.org/10.1093/he/9780192897381.001.0001
2. Hashmi, M.A.I., Butt, M.F., Jawad, M., & Sultan, S. Criminal Liability in the Age of Autonomous Systems: Rethinking Mens Rea and Actus Reus. — The Critical Review of Social Sciences Studies, Vol. 3, No. 3. 2025. https://doi.org/10.59075/szbtkr93
3. Sachoulido, A. AI Systems and Criminal Liability. — Oslo Law Review, Vol. 11, No. 1, 2024. — P. 1–10. https://doi.org/10.18261/olr.11.1.3
4. Abdelaziz, D.K.A. Criminal liability for the misuse and crimes committed by AI: A comparative analysis of legislation and international conventions. — Journal of Infrastructure, Policy and Development, 9(1), 2025. https://doi.org/10.24294/jipd10722
5. Hutapea, N.M.S. et al. Criminal Liability For AI-Based Cybercrime: Comparative Analysis Of Common Law And Civil Law Approaches. — Journal of Law, Politic and Humanities, 2025. https://dinastires.org/JLPH/article/view/2683
6. Abbott, R.B. & Sarch, A.F. Punishing Artificial Intelligence: Legal Fiction or Science Fiction. — UC Davis Law Review, Vol. 53, No. 1, 2019. https://doi.org/10.2139/ssrn.3327485
7. Rubinstein, D. Criminal liability for AI-caused harm: Mens Rea and beyond. — British Journal of Criminology, Vol. 62, No. 1, 2022. — P. 257–273. https://doi.org/10.1093/bjc/azab017
8. European Parliament. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). — Official Journal of the European Union, L 2024/1689, 12 July 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689
9. Council of Europe, CDPC. AI and Criminal Liability — Discussion Paper. CDPC (2024)09. — Strasbourg, 13 November 2024. https://rm.coe.int/cdpc-2024-09-ai-criminal-liability-discussion-paper-final-draft/1680b26f16
10. Arora, T. & Thakur, S. Criminal Liability of Artificial Intelligence: A Comprehensive Analysis of Legal Issues and Emerging Challenges. — International Journal of Research Publication and Reviews, Vol. 5, No. 11, 2024. — P. 1886–1891. https://www.researchgate.net/publication/397139159
11. Global Legal Insights. AI, Machine Learning & Big Data Laws and Regulations: China 2025. — ICLG, 2025. https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/china/
12. Hallevy, G. The Basic Models of Criminal Liability of AI Systems and Outer Circles. In: Moura Vicente, D., Soares Pereira, R. & Alves Leal, A. (eds.) Legal Aspects of Autonomous Systems: A Comparative Approach. Data Science, Machine Intelligence, and Law, Vol. 4. — Cham: Springer, 2024. — 381 p. — P. 69–82. https://doi.org/10.1007/978-3-031-47946-5_5
13. Iwannudin, I., Heriani, I. & Lestaluhu, R. Legal Challenges in Regulating Artificial Intelligence Use in Criminal Justice Systems. — Indonesia Law Reform Journal, Vol. 5, No. 2, July 2025. https://ejournal.umm.ac.id/index.php/ilrej/article/view/39901
14. Cambridge Forum on AI: Law and Governance. Generative AI and Criminal Law. — Cambridge Forum on AI: Law and Governance, 2025. https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governance/article/generative-ai-and-criminal-law/CFBB64250CAC6A338A5504F0F41C54AB

15. Taniady, V. AI-Induced Fatalities: A Criminal Law Perspective from Indonesia and International Perspective. — Journal of Law and Legal Reform, Vol. 6, No. 4, 2025. — P. 1805–1838. https://journal.unnes.ac.id/journals/jllr/article/view/35540

16. Simmler, M. Responsibility Gap or Responsibility Shift? The Attribution of Criminal Responsibility in Human–Machine Interaction. — Information, Communication & Society, Vol. 27, 2024. — P. 1142–1158. https://arxiv.org/pdf/2511.14964

Tadqiqot uz

ISSN 2181-9130

Doi Journal 10.26739/2181-9130

ҲУҚУҚИЙ ТАДҚИҚОТЛАР ЖУРНАЛИ

ЖУРНАЛ ПРАВОВЫХ ИССЛЕДОВАНИЙ

JOURNAL OF LAW RESEARCH

Taqdim etilayotgan maqolalarga qo‘yilgan talablar:

1. *Maqola o‘zbek, ingliz va rus tillarida qabul qilinadi va Microsoft Word dasturida Times New Roman shriftida 12 kegl, 1 satr oralig‘ida, sahifalar barcha tomondan 2 sm qoldirilgan bo‘lishi shart. Satr boshi - 1,25 sm bo‘lib, satrlarni eniga to‘g‘irlash, so‘zlarni boshqa qatorga ko‘chirish avtomatik tarzda bo‘lishi lozim.*
2. *Birinchi qator o‘ng tomondan muallifning familiyasi, ismi va otasining ismi, ikkinchi qatorda muallifning ish joyi, lavozimi, ilmiy darajasi va unvoni va e-mail, uchinchi qatorda sahafaning o‘rtasida bosh va qalin harflar bilan maqolaning nomi yoziladi. Ushbu ma’lumotlar o‘zbek, ingliz va rus tillarda berilishi lozim.*
3. *Keyingi qatordan o‘zbek, ingliz va rus tillarida kamida 60 ta o‘zbek, ingliz va rus tillarida so‘zdan iborat annotatsiya beriladi.*
4. *Keyingi qatordan 6-10 ta o‘zbek, ingliz va rus tillarida kalit so‘zlar beriladi.*
5. *Keyingi qatordan asosiy matn umimiy so‘zi minimal 2000 ta bo‘ladi.*
6. *Adabiyotlarning to‘liq ro‘yxati asosiy matndan so‘ng alifbo tartibida ko‘rsatilishi lozim va havolalar asosiy matnda bo'lishi kerak [1, B.25].*
7. *Maqolada keltirilgan dalillarning to‘g‘riligi uchun muallif mas’ul, plagiat holati taqiqlanadi.*
8. *Web of science, Scopus tizimidagi jurnallardan iqtiboslar olish maqsadga muvofiqdir.*

Требования к оформлению научной статьи:

1. *Статья принимается на узбекском, английском и русском языках и должна быть оформлена в Microsoft Word шрифтом Times New Roman, размер 12, межстрочный интервал — 1, поля со всех сторон — 2 см. Абзацный отступ — 1,25 см; выравнивание по ширине и переносы слов должны быть включены автоматически.*
2. *В первой строке справа указываются фамилия, имя и отчество автора; во второй строке — место работы автора, должность, ученая степень и звание, а также e-mail; в третьей строке по центру страницы крупным и жирным шрифтом — название статьи. Эти сведения должны быть приведены на узбекском, английском и русском языках.*
3. *Ниже дается аннотация на узбекском, английском и русском языках, содержащая не менее 60 слов на каждом языке.*
4. *Далее приводятся 6–10 ключевых слов на узбекском, английском и русском языках.*
5. *Далее основной текст: общий объем текста должен быть не менее 2000 слов.*
6. *Полный список литературы должен быть приведен после основного текста в алфавитном порядке; ссылки должны присутствовать в основном тексте в формате [1, С.25].*
7. *Автор несет ответственность за достоверность приведенных в статье доказательств; плагиат запрещен.*
8. *Рекомендуется цитирование журналов из база данных Web of Science и Scopus.*

Requirements of the articles submitted:

1. *Articles are accepted in Uzbek, English and Russian and must be prepared in Microsoft Word using Times New Roman font, size 12, single line spacing, with 2 cm margins on all sides. First-line indent is 1.25 cm; text should be justified and word hyphenation/line breaks set to automatic.*
2. *In the first line on the right: the author’s surname, given name and patronymic; in the second line: the author’s affiliation, position, academic degree and title, and e-mail; in the third line centered on the page: the article title in bold and uppercase (or bold). These details must be provided in Uzbek, English and Russian.*
3. *Next, provide an abstract in Uzbek, English and Russian of at least 60 words in each language.*
4. *Next, provide 6–10 keywords in Uzbek, English and Russian.*
5. *Next, the main text: total word count must be at least 2000 words.*
6. *The full list of references must appear after the main text in alphabetical order, and citations should appear in the main text in the format [1, P.25].*
7. *The author is responsible for the accuracy of the evidence presented in the article; plagiarism is prohibited.*
8. *It is advisable to include citations from journals indexed in Web of Science and Scopus.*