Artificial Intelligence and the Criminal Justice System: An Analysis of Liabilities and Consequences

1. Ardeshir Jafarnejad Sani *: Department of Law, Cha.C., Islamic Azad University, Chalus, Iran

*Correspondence: ardeshirjafarnezhad70@iau.ac.ir

Abstract

Artificial intelligence has become an influential technological force in contemporary criminal justice systems, reshaping criminal investigation, evidence analysis, predictive policing, sentencing, surveillance, cybercrime prevention, and institutional decision-making. This article analyzes the legal responsibilities and consequences arising from the use and misuse of artificial intelligence within the criminal justice system. The central problem addressed is whether traditional criminal law doctrines, which are historically based on human agency, intention, culpability, causation, and punishment, can adequately respond to autonomous or semi-autonomous AI systems that generate harmful, biased, or legally significant outcomes. Using a doctrinal, analytical, and interdisciplinary approach, the article examines the theoretical foundations of AI and criminal law, the liability of developers, programmers, users, operators, corporations, and public institutions, and the controversial question of whether AI itself can be treated as a subject of criminal liability. The analysis argues that direct criminal liability of AI remains conceptually weak because criminal punishment presupposes moral agency, consciousness, and blameworthiness. Instead, a layered model of responsibility is proposed, based on human and corporate accountability, foreseeability, control, negligence, compliance duties, and institutional oversight. The article also evaluates the broader consequences of AI for criminal justice, including algorithmic discrimination, opacity, privacy violations, mass surveillance, evidentiary uncertainty, due process risks, and the possible dehumanization of justice. At the same time, it recognizes AI's potential benefits in improving investigative efficiency, detecting cybercrime, managing complex evidence, and supporting judicial administration. The article concludes that artificial intelligence should not be rejected from criminal justice, but its use must be strictly regulated through transparency, explainability, human oversight, anti-discrimination safeguards, auditability, and effective remedies. A human-centered legal framework is necessary to ensure that technological innovation strengthens rather than undermines accountability, fairness, and the moral legitimacy of criminal justice.

Keywords: Artificial Intelligence; Criminal Justice System; Criminal Liability; Algorithmic Accountability; AI Governance; Due Process; Algorithmic Discrimination; Legal Responsibility.

Received: 01 January 2026
Revised: 17 May 2026
Accepted: 24 May 2026
Initial Publish: 24 May 2026
Final Publish 01 September 2026

Copyright: © 2026 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Citation: Jafarnejad Sani, A. (2026). Artificial Intelligence and the Criminal Justice System: An Analysis of Liabilities and Consequences. *Legal Studies in Digital Age,* 5(5), 1-14.

1. Introduction

Artificial intelligence has moved from the margins of technological speculation into the core of contemporary legal, administrative, and criminal justice systems. Its development has affected not only private markets and digital platforms but also the institutional practices through which states investigate crime, assess risk, manage security, classify offenders, evaluate evidence, and distribute punishment. In this context, the criminal justice system is no longer a purely human-centered institutional field; it is increasingly mediated by algorithmic tools, predictive analytics, automated classification systems, facial recognition technologies, digital forensic infrastructures, and AI-supported decision-making mechanisms. This transformation creates a fundamental legal question: whether doctrines designed for human conduct, intentionality, culpability, negligence, causation, and punishment can adequately respond to systems that learn, adapt, operate probabilistically, and sometimes produce outcomes that neither designers nor users fully anticipated. The expansion of AI in criminal justice management has therefore generated a broad field of inquiry concerned with both operational efficiency and normative legitimacy, especially because AI is increasingly discussed as a tool for policing, sentencing, prison administration, cybercrime prevention, and legal decision support (Talukder & Shompa, 2024). The central difficulty is that criminal law is historically structured around human agency, while AI systems are often evaluated through concepts such as autonomy, opacity, data dependency, algorithmic inference, and systemic risk (Karnouskos, 2021). As a result, the legal system faces not merely a technical problem but a conceptual disruption in the meaning of responsibility, control, and accountability.

The increasing dependence of criminal justice institutions on AI reflects the broader digitalization of law and governance. Digital systems have introduced new modes of legal reasoning, administrative classification, and evidentiary processing, and the use of AI has intensified these developments by allowing institutions to process immense volumes of data, identify patterns, and generate predictions that would be difficult for human actors to produce manually. Scholars have emphasized that algorithms are no longer external instruments used by legal actors; rather, they increasingly participate in the formation of legal outputs, administrative risk scores, and institutional judgments (Losavio, 2021). This shift has particular importance in criminal law because the consequences of error are severe: wrongful suspicion, discriminatory surveillance, unjustified detention, disproportionate sentencing, or the erosion of due process guarantees. The legal significance of AI therefore cannot be reduced to its technological efficiency. Even where AI improves speed or analytical capacity, it raises questions about transparency, contestability, explainability, and the ability of affected persons to understand or challenge decisions made about them (Cheong, 2024). In criminal justice, where liberty, dignity, reputation, and state coercion are at stake, these questions become central to the legitimacy of legal authority.

The problem becomes more complex when AI is not merely used by criminal justice institutions but becomes involved in the commission of crimes. AI can be used as an instrument for fraud, identity theft, cyberattacks, deepfake extortion, automated market manipulation, illegal surveillance, and other digitally mediated offenses. The criminal misuse of AI has therefore become a major concern in contemporary legal scholarship, particularly because existing criminal frameworks may be insufficient when harmful outcomes are produced through autonomous, semi-autonomous, or opaque technological systems (S et al., 2024). Cybersecurity scholarship has similarly emphasized that AI expands both defensive and offensive capabilities, creating new questions about who should be culpable when intelligent systems are deployed to cause harm or when negligent design enables criminal exploitation (Chaturvedi & Tiwari, 2023). These questions are particularly challenging because the harm may result from multiple interacting actors, including developers, data suppliers, corporate owners, operators, users, and third-party malicious agents. The attribution of liability is therefore fragmented across technical, organizational, and human components, which complicates conventional criminal law doctrines based on identifiable conduct, mental state, and causal connection.

At the theoretical level, AI challenges the anthropocentric assumptions of criminal responsibility. Traditional criminal law presupposes that culpability is attached to a human person who acts voluntarily, understands or should understand the wrongful nature of conduct, and can be punished in a meaningful way. Yet AI systems may perform actions that appear decision-like without possessing consciousness, moral understanding, or human intentionality. This has led to debates over whether AI can or should be treated as a legal subject, whether punishment of AI is merely a fiction, and whether responsibility should remain exclusively with human or corporate actors (Abbott & Sarch, 2024). Some discussions of electronic liability and international

crimes have gone further by questioning whether the individual-centered framework of criminal law can adequately address harms produced by complex digital systems (Swart, 2023). However, attributing criminal personality to AI remains deeply controversial because criminal punishment is traditionally linked to moral blameworthiness, deterrence, rehabilitation, and expressive condemnation, all of which presuppose capacities that AI does not possess in the human sense. The problem is therefore not only whether AI can be punished but whether criminal law should reconfigure responsibility around networks of control, design, deployment, and governance.

The issue also has a comparative and international dimension. Different legal systems are beginning to respond to AI through regulatory, administrative, civil, and criminal mechanisms, but these responses remain uneven. European legal discourse has been especially active in addressing the permissibility of AI use in criminal matters while attempting to preserve fundamental rights and procedural guarantees (Ivan & Manea, 2022). In France, recent legal developments have shown how national systems attempt to situate AI within broader digital law and regulatory modernization (Duflot, 2024). International governance debates similarly emphasize both opportunities and challenges, especially because AI systems cross borders, operate through global data infrastructures, and can affect international law, security, and institutional accountability (Ness et al., 2024). These developments show that the AI-criminal justice relationship cannot be analyzed solely within domestic criminal law. It also involves international legal coordination, comparative regulatory learning, human rights norms, cybersecurity standards, corporate governance, and technological ethics.

The normative stakes of this inquiry are particularly serious because AI may reproduce, intensify, or conceal structural inequalities. Algorithmic discrimination has become a central issue in AI regulation, especially where training data reflects historical bias or where predictive models generate unequal outcomes for different social groups (Wang et al., 2024). In criminal justice, biased algorithmic systems can reinforce discriminatory policing, unequal sentencing, and selective surveillance. This risk is not hypothetical, because criminal justice institutions often rely on historical crime data, arrest records, neighborhood-level risk indicators, and administrative datasets that may already reflect unequal enforcement patterns. If such data is used without critical safeguards, AI systems may convert past injustice into apparently objective prediction. Ethical analyses of AI therefore stress the importance of fairness, accountability, explainability, privacy, human oversight, and the prevention of harm (Stahl, 2021). Human rights scholarship has similarly argued that AI must be assessed through principles such as equality, dignity, non-discrimination, and access to justice, especially where automated systems affect vulnerable populations (Chatterjee & N.S, 2021).

This article examines artificial intelligence and the criminal justice system through an analytical legal framework focused on liabilities and consequences. It proceeds from the premise that AI does not merely create new tools for criminal justice but also destabilizes foundational assumptions of criminal responsibility. It analyzes the conceptual foundations of AI and criminal law, the liability of developers, users, operators, corporations, and potentially autonomous systems, the consequences of AI for criminal justice institutions and fundamental rights, and the need for regulatory frameworks capable of reconciling technological innovation with legal accountability. The objective of this study is to analyze the liabilities and consequences arising from the use and misuse of artificial intelligence in the criminal justice system and to propose a legally coherent framework for preserving accountability, fairness, and human-centered justice in the age of algorithmic decision-making.

2. Theoretical and Conceptual Foundations of Artificial Intelligence and Criminal Law

Artificial intelligence is not a single technology but a broad category of computational systems designed to perform tasks that normally require human-like cognitive functions, including classification, prediction, recognition, optimization, natural language processing, and decision support. In legal and criminal justice contexts, the most relevant forms of AI are not speculative forms of artificial general intelligence but practical systems based on machine learning, data analytics, neural networks, automated reasoning, and algorithmic modeling. These systems operate by identifying patterns in data and producing outputs that may influence institutional decisions. This creates a complex relationship between AI and law because criminal law depends on categories such as act, omission, intention, negligence, capacity, causation, and blameworthiness, while AI systems are structured around probabilistic inference, data-driven learning, and technical optimization. Legal scholarship on law, robots, and society has therefore emphasized that AI creates a form of human-machine symbiosis in which human actors

increasingly depend on artificial systems while still needing to preserve legal responsibility and social control (Karnouskos, 2021). This interaction is especially significant in criminal justice, where technologies may affect the identification of suspects, the assessment of danger, the interpretation of evidence, and the allocation of punitive consequences.

The conceptual foundation of criminal law rests on the distinction between wrongful conduct and culpable mental state. The traditional structure of criminal responsibility requires a prohibited act or omission, a legally relevant mental element, and a causal connection between conduct and harm. AI disrupts this structure because the immediate operational act may be performed by a machine, while the mental state belongs, if at all, to one or more human actors who designed, trained, deployed, supervised, or misused the system. In the context of AI and autonomous vehicles, comparative criminal law analysis has shown that negligence becomes a crucial doctrinal category because many AI-related harms may arise not from direct intention but from failures of design, testing, monitoring, warning, or intervention (Giannini & Kwik, 2023). The same reasoning applies to criminal justice technologies. If a predictive policing algorithm disproportionately targets a community because of biased data, the immediate output is generated by the system, but legal analysis must investigate the human and institutional choices embedded in data selection, model design, validation, deployment, and reliance. Criminal law therefore has to move beyond the visible moment of harm and examine the chain of human decisions that made the AI outcome possible.

The theoretical challenge also concerns autonomy. AI systems may be described as autonomous when they can operate without continuous human instruction, adapt to new data, or generate outputs not explicitly pre-programmed by developers. However, legal autonomy is not the same as technical autonomy. A machine may be operationally autonomous without being morally autonomous. This distinction is vital because criminal responsibility traditionally presupposes a subject capable of understanding norms, forming intentions, and responding to blame. Philosophical and legal discussions of responsibility gaps have identified several areas where AI complicates accountability: it may be unclear who caused the harm, who could have prevented it, who had meaningful control, and who can justifiably be blamed (Sio & Mecacci, 2021). These gaps are not merely theoretical abstractions. They may appear when a criminal justice agency relies on an AI tool that produces an erroneous risk score, when a company deploys a defective security algorithm that enables cybercrime, or when an autonomous weapon system selects targets in a manner inconsistent with international criminal law. In each case, the law must decide whether liability should attach to the operator, designer, commander, corporation, public authority, or some combination of actors.

Another foundation of the AI-criminal law relationship is the principle of legality. Criminal law generally requires that offenses and penalties be defined clearly in advance, so individuals can know what conduct is prohibited. AI challenges legality in two ways. First, AI creates new forms of conduct that existing criminal statutes may not clearly anticipate, such as AI-generated impersonation, automated fraud, synthetic evidence manipulation, or autonomous cyber intrusion. Second, AI introduces uncertainty into legal decision-making when algorithmic tools influence judicial or administrative outcomes without transparent reasoning. In the digital environment, criminal participation models must be reexamined because harmful conduct may be distributed across platforms, software systems, remote users, and automated agents (Piparo, 2023). This distribution complicates the identification of perpetrators, accomplices, facilitators, and negligent enablers. It also creates difficulties for procedural fairness, because defendants may need access to algorithmic logic or training data to challenge the evidentiary or predictive basis of a criminal justice decision.

The relationship between AI and criminal law is also shaped by the difference between using AI as an instrument of crime and using AI as an instrument of criminal justice. When AI is used as an instrument of crime, the legal focus is on criminal misuse, culpable deployment, and the liability of those who intentionally or recklessly exploit technological systems. The emergence of AI-supported cybercrime illustrates this point, because malicious actors can use AI to automate attacks, generate deceptive content, evade detection, or scale fraudulent conduct (Velasco, 2022). When AI is used as an instrument of criminal justice, however, the legal focus shifts to institutional accountability, procedural safeguards, and rights protection. AI tools in criminal justice may assist with case management, forensic analysis, risk assessment, sentencing recommendations, and administrative efficiency, but their use must be constrained by due process and fundamental rights (Muthukuda Arachchige Dona Shiroma Jeeva Shirajanie, 2024). The same technology can therefore serve both public security and criminal harm, depending on its design, governance, and use.

A further conceptual issue concerns legal personality. Some scholars have debated whether AI systems should receive a limited form of legal status, especially where they act independently and cause legally significant harm. Islamic jurisprudential

analysis of AI legal capacity, for example, raises questions about whether artificial systems can be analogized to recognized legal subjects or whether capacity remains necessarily tied to human attributes (Sitiris & Busari, 2024). In secular legal theory, similar debates appear in discussions of electronic personhood and AI punishment. Arguments in favor of limited AI legal personality often rely on functional considerations, such as accountability, compensation, or regulatory clarity. Arguments against it emphasize that legal personality may obscure human responsibility by allowing corporations, developers, or users to shift blame onto machines. This concern is especially strong in criminal law, where liability must not become a symbolic fiction that weakens accountability for those who design and deploy harmful systems. Thus, even if AI is treated as a legal object or regulatory entity, it does not follow that it should be treated as a criminal subject capable of guilt.

The concept of algorithmic opacity is central to the theoretical framework. Many AI systems, especially complex machine learning models, are difficult to explain even for their designers. This opacity creates a "black box" problem in criminal justice because affected persons may not understand how a decision was reached, and courts may struggle to evaluate reliability, bias, and causation. Transparency and accountability have therefore become core legal values in the governance of AI systems (Cheong, 2024). Yet transparency is not simply a technical requirement; it is a legal condition for contestability, judicial review, and procedural fairness. If a defendant cannot examine the basis of an algorithmic risk assessment, the right to challenge evidence may be weakened. If a judge relies on a proprietary sentencing tool without understanding its assumptions, judicial discretion may become dependent on private technological infrastructure. If police agencies use predictive models without public oversight, surveillance may expand without democratic control. These scenarios show that AI affects not only substantive criminal law but also criminal procedure and institutional legitimacy.

Ethics also forms part of the theoretical foundation because criminal justice is not merely a system of rule application; it is a coercive moral and political institution. AI ethics emphasizes fairness, non-maleficence, accountability, autonomy, transparency, and social responsibility (Mensah, 2024). These principles overlap with legal values but do not replace them. Criminal law requires enforceable norms, procedural rights, and institutional accountability, while ethics provides broader evaluative criteria for responsible design and deployment. The ethical issues of AI are especially acute where systems classify human beings, assess risk, or recommend punitive measures (Stahl, 2021). Even if an AI system is statistically accurate at an aggregate level, its use may still be unjust if it undermines dignity, reinforces bias, denies individualized assessment, or prevents meaningful human review. Criminal justice must therefore treat AI not simply as a neutral technology but as an institutional actor whose outputs are shaped by data, design choices, legal incentives, and social power.

The theoretical foundations of AI and criminal law therefore reveal a deep tension between technological functionality and legal normativity. AI systems can increase efficiency, identify hidden patterns, and support decision-making, but they also create responsibility gaps, legality problems, opacity, discrimination risks, and challenges to human-centered culpability. Legal systems must avoid two extremes. One extreme is technological enthusiasm, which assumes that AI can improve criminal justice without altering its normative foundations. The other extreme is technological rejection, which ignores the practical reality that AI is already embedded in criminal justice systems and will continue to shape legal practice. A more defensible approach recognizes that AI must be integrated into criminal law only under conditions of accountability, explainability, human oversight, proportionality, and rights protection. This approach provides the theoretical basis for analyzing liability in AI systems and for evaluating the broader consequences of AI in criminal justice.

3. Criminal Liability and Responsibility in Artificial Intelligence Systems

The most difficult issue in the legal analysis of artificial intelligence and criminal justice is the attribution of criminal liability. Criminal responsibility depends on the identification of a responsible subject, a prohibited act or omission, a mental element, and a causal relationship between conduct and harm. AI complicates each of these elements because harmful outcomes may result from the interaction of data, code, autonomous learning, corporate deployment, user behavior, institutional reliance, and environmental conditions. In traditional criminal law, a person who uses a tool to commit a crime remains responsible because the tool is passive. AI systems, however, may not be passive in the same sense. They can process information, adjust outputs, and operate in ways not fully predictable at the time of deployment. This has led scholars to question whether existing doctrines can adequately capture AI-related culpability or whether criminal law must develop new models of distributed responsibility (Karchevskyi & Radutniy, 2023). The central point is not that AI should automatically become a criminal

subject, but that criminal law must become capable of tracing responsibility across complex technological systems without dissolving blame into technical uncertainty.

The first and most direct category of liability concerns developers and programmers. Developers may bear responsibility when harm results from defective design, unsafe coding, inadequate testing, foreseeable misuse, or failure to incorporate safeguards. In many AI systems, the developer's contribution is not limited to writing code; it includes selecting training data, defining objectives, choosing model architecture, setting risk thresholds, validating outputs, and anticipating deployment environments. If an AI system used in criminal justice produces discriminatory or dangerous results because developers ignored known risks, the issue may be framed as negligence, recklessness, or, in extreme cases, knowing facilitation of harm. Comparative analysis of AI and autonomous vehicles shows that negligence-based frameworks can be adapted to AI where liability is tied to failures in precaution, monitoring, and correction (Giannini & Kwik, 2023). However, negligence doctrine must be refined for AI because foreseeability is difficult when machine learning systems evolve through data interaction. The law must therefore ask not only whether a specific harm was foreseeable, but whether the category of harm was foreseeable in light of the system's design, data limitations, and intended use.

The liability of users and operators forms the second major category. AI systems are often deployed by individuals, police agencies, corporations, prosecutors, judges, military actors, or administrative bodies. These actors may use AI lawfully, negligently, recklessly, or intentionally for harmful purposes. Where a person intentionally uses AI to commit fraud, generate false evidence, automate harassment, or conduct cyber intrusion, AI functions as an instrument of crime, and ordinary principles of criminal liability can apply. Recent discussions of legal frameworks for criminal misuse of AI emphasize that the criminal law must clearly address intentional exploitation of AI tools, particularly where AI increases the scale, speed, or concealment of criminal conduct (S et al., 2024). However, more difficult cases arise when operators rely on AI outputs without sufficient supervision. A criminal justice agency may use a risk assessment tool that produces biased recommendations; a judge may give weight to an opaque sentencing algorithm; a police department may use predictive policing software without auditing its discriminatory impact. In such cases, liability may arise not from malicious intent but from negligent reliance, institutional omission, or failure to preserve human judgment.

Corporate criminal liability is especially important because many AI systems are developed, owned, licensed, and maintained by companies. Technology companies may profit from systems used in policing, surveillance, cybersecurity, sentencing, border control, or data analysis, while also controlling access to source code, model documentation, and performance data. Corporate misconduct in algorithmic systems has been analyzed as a distinct category of harm because organizational decisions may create risks that cannot be reduced to the conduct of a single employee (Diamantis, 2021). In this sense, AI-related harm may result from corporate culture, inadequate compliance systems, commercial pressure, secrecy, insufficient auditing, or reckless deployment of immature technology. Corporate criminal responsibility becomes especially relevant where a company markets a system as reliable despite knowing its limitations, fails to disclose error rates, ignores discriminatory outcomes, or designs AI tools in ways that foreseeably facilitate illegal use. The doctrine of corporate criminal liability can therefore serve as a bridge between individual culpability and systemic technological harm.

The economic and financial sector provides an important analogy for AI-related criminal responsibility. AI can be used to prevent fraud, detect suspicious transactions, and improve compliance, but it can also facilitate economic and financial crime through automated manipulation, concealment, and complex digital transactions. Studies of AI in the economic sector emphasize both prevention and accountability, showing that intelligent systems can support regulatory compliance while simultaneously creating new risks of misuse (Rodrigues, 2021). In relation to corporate criminal responsibility, compliance and AI are intertwined because organizations increasingly use AI to monitor legal risk, detect wrongdoing, and manage internal controls (Rodrigues et al., 2021). However, the use of AI in compliance does not absolve corporations of responsibility. If a company adopts AI compliance tools merely as symbolic protection, ignores warning signals, or designs systems that prioritize profit over legality, AI may become part of the mechanism of wrongdoing rather than a safeguard against it. Criminal law must therefore evaluate the actual governance function of AI, not merely its formal adoption.

The question of direct AI liability remains highly controversial. Some scholars argue that AI may eventually require legal recognition as a responsible entity, especially where its decisions are highly autonomous and not reducible to individual human intent. The idea of punishing artificial intelligence has been explored as either a legal fiction or a speculative extension of

criminal responsibility (Abbott & Sarch, 2024). Yet the direct punishment of AI faces fundamental objections. AI lacks consciousness, moral understanding, suffering, and human dignity; it cannot experience blame, remorse, deterrence, or rehabilitation in the human sense. Punishing AI may therefore be symbolically incoherent and practically dangerous if it allows human or corporate actors to avoid responsibility. At most, sanctions directed at AI systems may take regulatory forms, such as deactivation, modification, seizure, certification withdrawal, or operational restriction. These are not punishments in the traditional criminal sense but preventive or administrative measures. Criminal law should therefore be cautious about granting AI criminal personality, because doing so may weaken the normative connection between culpability and human agency.

International criminal law intensifies the problem of AI liability, especially in relation to autonomous weapons systems. Autonomous weapons controlled by AI raise questions about responsibility for unlawful targeting, civilian harm, command responsibility, and compliance with international humanitarian law (Acquaviva, 2022). Similar concerns arise in broader discussions of autonomous weapon systems under international law, where the delegation of lethal decision-making to machines challenges principles of distinction, proportionality, necessity, and human control (Akkuş, 2022). If an autonomous system commits an act that would constitute a war crime if performed by a human soldier, responsibility may potentially attach to commanders, programmers, manufacturers, state officials, or operators, depending on knowledge, control, foreseeability, and failure to prevent harm. Electronic liability for international crimes has been proposed as a way to transcend purely individual models, but such proposals remain controversial because international criminal law is fundamentally organized around individual accountability (Swart, 2023). The challenge is to avoid impunity without inventing fictional responsibility that obscures the human and institutional decisions behind AI deployment.

Causation is another major obstacle in AI-related criminal liability. In conventional criminal law, causation requires a connection between conduct and prohibited result. In AI systems, causation may be distributed across the life cycle of development and deployment. A harmful outcome may result from biased data collected years earlier, design choices made by a development team, inadequate testing by a company, negligent procurement by a public agency, improper use by an operator, and unpredictable adaptation by the model. Responsibility gaps arise when no single actor appears to satisfy the full requirements of actus reus and mens rea, even though the overall system produced serious harm (Sio & Mecacci, 2021). Criminal law must therefore develop methods for evaluating causal contribution in complex socio-technical systems. This may include duties of documentation, audit trails, explainability requirements, and mandatory human oversight. Without these mechanisms, it may be impossible to reconstruct how an AI system produced a harmful output, which would undermine both prosecution and defense rights.

Evidentiary problems are closely related to causation. AI systems may generate evidence, classify evidence, detect patterns, or produce expert-like outputs. However, if the system is opaque, proprietary, or technically complex, courts may struggle to determine reliability. The use of AI by lawyers and legal professionals has already raised questions about competence, transparency, and professional responsibility (Świerczyński, 2021). In criminal proceedings, these concerns are heightened because defendants must be able to challenge evidence used against them. If AI-generated evidence cannot be explained, tested, or independently verified, its use may conflict with fair trial guarantees. Anti-fraud laws may even complicate legitimate computer science research by restricting the ability of researchers to test systems, identify vulnerabilities, or expose weaknesses (Xiao et al., 2025). This creates a paradox: legal rules intended to prevent digital wrongdoing may hinder the very research needed to make AI systems safer and more accountable. Criminal justice systems must therefore distinguish malicious interference from good-faith security research and algorithmic accountability work.

A further dimension of liability concerns public institutions that adopt AI tools. Criminal justice authorities cannot outsource constitutional and legal duties to algorithms. If a court, police agency, or correctional institution relies on AI, it must ensure that the system is lawful, reliable, explainable, non-discriminatory, and subject to human review. AI use in criminal matters under EU law has been discussed in terms of preserving the essence of fundamental rights, which means that efficiency cannot justify the erosion of procedural protections (Ivan & Manea, 2022). In sentencing contexts, AI may offer opportunities for consistency and data-informed analysis, but it may also threaten individualized justice if judges defer excessively to algorithmic outputs (Muthukuda Arachchige Dona Shiroma Jeeva Shirajanie, 2024). Public authorities should therefore remain accountable for decisions made with AI assistance, even where technical systems are developed by private vendors. The final

legal decision must remain attributable to a human institution capable of giving reasons, hearing objections, and correcting error.

Criminal liability in AI systems therefore requires a layered approach. Developers may be liable for defective design or negligent safeguards; users may be liable for intentional misuse or reckless reliance; corporations may be liable for organizational misconduct; public institutions may be liable for unlawful deployment; commanders may be liable for autonomous weapons misuse; and AI systems themselves may be subject to regulatory restrictions rather than true punishment. The most defensible model is not direct criminal liability of AI but distributed human and corporate accountability organized around control, foreseeability, benefit, duty, and preventability. This model preserves the moral structure of criminal law while adapting it to complex technological systems. It recognizes that AI can generate novel risks, but it refuses to allow technological complexity to become a shield against responsibility.

4. Consequences, Risks, and Impacts of Artificial Intelligence on the Criminal Justice System

Artificial intelligence produces both opportunities and dangers for the criminal justice system. Its positive consequences are often emphasized in policy debates: faster investigations, more efficient case management, improved data analysis, enhanced detection of digital crime, better allocation of police resources, and potential reduction of human error. AI systems can process large volumes of evidence, detect patterns in financial transactions, identify cyber threats, support forensic analysis, translate or classify documents, and assist in the management of complex criminal cases. Systematic literature on AI in criminal justice management shows that AI is often presented as a tool for improving institutional efficiency and operational capacity (Talukder & Shompa, 2024). In cybercrime contexts, AI can assist law enforcement agencies in detecting malicious activity, identifying suspicious network behavior, and responding to technologically sophisticated offenses (Velasco, 2022). These advantages are significant because contemporary crime is increasingly digital, transnational, data-intensive, and technically complex. Without advanced technological tools, criminal justice institutions may struggle to respond effectively to cybercrime, automated fraud, digital exploitation, and AI-enabled offenses.

However, the benefits of AI must be assessed against the risks of algorithmic error, bias, and institutional overreliance. In criminal justice, an inaccurate AI output can have severe consequences. A false match in facial recognition may lead to wrongful suspicion; a biased risk score may influence pretrial detention; an opaque sentencing recommendation may increase punishment; a flawed predictive policing model may intensify surveillance in already over-policed communities. Algorithmic discrimination is therefore one of the most serious consequences of AI adoption, particularly because discrimination may arise from data, design, proxy variables, model objectives, or institutional use (Wang et al., 2024). The danger is not only that AI may discriminate, but that its discrimination may appear neutral because it is expressed through numbers, risk scores, probabilities, or technical outputs. This appearance of objectivity may make discriminatory decisions harder to detect and challenge. In criminal justice, where affected persons may already face social, economic, or political vulnerability, algorithmic discrimination can deepen structural inequality under the guise of technological modernization.

The risk of opacity compounds the problem of discrimination. If an AI system produces a recommendation without clear explanation, neither the defendant nor the judge may understand why the system reached its conclusion. Transparency and accountability are therefore essential to safeguarding well-being and justice in algorithmic decision-making (Cheong, 2024). Yet transparency must be meaningful rather than formal. It is not enough to disclose that AI was used; affected persons must be able to understand the basis of the decision in a way that allows contestation. This requires information about data sources, error rates, validation methods, model assumptions, and the role of human decision-makers. In criminal justice, explainability is linked to due process. A person cannot effectively challenge an algorithmic decision if the logic of that decision is hidden behind proprietary secrecy or technical complexity. Courts must therefore ensure that AI-assisted evidence and decisions remain reviewable, interpretable, and subject to adversarial scrutiny.

AI also affects the presumption of innocence. Predictive systems often operate by estimating the probability of future behavior based on patterns in past data. In criminal justice, this can shift attention from proven conduct to predicted risk. While risk assessment has long existed in law, AI intensifies its reach by making prediction appear more precise, scientific, and administratively attractive. This can produce a preventive logic in which individuals are treated as dangerous because of statistical associations rather than established wrongdoing. The use of AI in sentencing illustrates this tension: AI can support

consistency and identify relevant patterns, but it may also reduce individualized judgment and embed social bias into punitive decision-making (Muthukuda Arachchige Dona Shiroma Jeeva Shirajanie, 2024). The criminal justice system must therefore distinguish between using AI as an informational aid and allowing AI to determine punishment. If prediction becomes a substitute for proof or individualized assessment, the legitimacy of criminal justice is weakened.

Privacy is another major consequence of AI in criminal justice. AI systems often require large datasets, including biometric data, location data, communication metadata, social media information, financial records, and behavioral patterns. The expansion of AI-based surveillance can create a criminal justice environment in which individuals are continuously monitored, classified, and scored. Human rights scholarship warns that AI must be evaluated through legal and policy frameworks that protect dignity, privacy, equality, and fundamental freedoms (Chatterjee & N.S, 2021). These concerns are particularly acute where AI is used by the state because criminal justice authorities possess coercive power. Surveillance technologies may be justified by security needs, but without strict limits they can normalize intrusive monitoring and undermine democratic freedoms. AI therefore creates a risk of digital authoritarianism when predictive analytics, biometric identification, and automated surveillance are used without transparency, judicial control, or effective remedies.

Public trust is also affected by the use of AI. Criminal justice institutions depend on legitimacy, and legitimacy depends on the perception that decisions are fair, reasoned, accountable, and humanly understandable. If people believe that criminal justice decisions are being made by opaque machines or by public officials who cannot explain their reliance on technology, trust may decline. Public perceptions of AI implementation are important because social acceptance depends not only on technical performance but also on confidence, fairness, and the perceived appropriateness of AI in sensitive domains (Romero & Young, 2021). Criminal justice differs from many administrative fields because its decisions involve punishment, stigma, coercion, and deprivation of liberty. Even a technically accurate system may be socially unacceptable if it appears to remove human judgment from morally significant decisions. The challenge is therefore not simply to make AI more accurate, but to ensure that its use remains compatible with public expectations of justice.

AI also changes the role of legal professionals. Lawyers, judges, prosecutors, and police officers may increasingly depend on AI tools for research, evidence analysis, case prediction, drafting, and risk evaluation. The use of AI in legal work raises questions about professional responsibility, competence, confidentiality, and independent judgment (Świerczyński, 2021). In criminal justice, defense lawyers may need technical expertise to challenge algorithmic evidence; prosecutors may need standards for disclosing AI-assisted investigative methods; judges may need training to assess AI reliability; and police agencies may need governance protocols for algorithmic tools. If legal professionals lack the ability to understand or question AI systems, they may defer to technological outputs in ways that undermine their institutional duties. Therefore, AI requires not only new laws but also new professional capacities within the criminal justice system.

AI-enabled criminality is another major consequence. The same tools that assist law enforcement can empower offenders. AI can generate phishing messages, deepfake evidence, synthetic identities, automated hacking strategies, malware adaptation, and disinformation campaigns. The culpability question becomes difficult when AI tools are open-source, widely available, or embedded in general-purpose platforms. Cybersecurity scholarship asks who should be culpable in the age of AI when harmful outcomes may result from malicious users, insecure systems, negligent providers, or autonomous adaptation (Chaturvedi & Tiwari, 2023). This issue is especially important because AI can scale crime. A single offender using AI may target thousands of victims, automate deception, and conceal identity more effectively than traditional offenders. Criminal law must therefore respond to the amplification effect of AI, while avoiding overly broad criminalization that may suppress legitimate research, innovation, or ordinary technological use.

The consequences of AI also extend to international governance and cross-border crime. AI systems operate through global infrastructures, and AI-enabled crimes often cross jurisdictions. A cyberattack may be launched from one country, use servers in another, target victims in several others, and rely on AI tools developed by multinational companies. International legal and governance scholarship emphasizes that AI creates both opportunities and challenges for international law, including questions of coordination, sovereignty, accountability, and regulatory fragmentation (Ness et al., 2024). The international dimension is especially important for cybercrime, autonomous weapons, financial crime, and transnational surveillance. Without cooperation, states may develop inconsistent rules, creating enforcement gaps and safe havens for AI-enabled criminal activity.

At the same time, international cooperation must respect human rights and avoid becoming a justification for excessive surveillance or cross-border repression.

There are also consequences for access to justice. AI can potentially assist legal research, simplify procedures, translate legal information, and support under-resourced institutions. However, it can also create new inequalities if only powerful institutions have access to advanced AI tools while defendants, marginalized communities, or small legal practices lack equivalent resources. Digital justice can therefore reproduce unequal power relations unless access, transparency, and contestability are built into AI governance. The idea of justice in a digital world requires attention to both old legal problems and new technological challenges (BĂDescu, 2023). AI does not eliminate traditional concerns about fairness, inequality, state power, and legal protection; rather, it reconfigures them in a digital environment. The criminal justice system must therefore ensure that AI does not become a mechanism through which efficiency is achieved at the expense of equality and defense rights.

The broader consequence of AI is the possible dehumanization of criminal justice. Criminal law is not merely a system for calculating risk; it is a normative institution that condemns wrongdoing, recognizes responsibility, protects rights, and expresses social judgment. If AI shifts criminal justice toward prediction, classification, and optimization, the system may lose sight of human dignity, moral agency, and individualized justice. Ethical analyses of AI warn that technical systems must be evaluated in relation to human values and social consequences (Stahl, 2021). AI should therefore support, not replace, human judgment in criminal justice. The goal should not be to automate punishment but to improve legal reasoning, evidence analysis, and institutional accountability under human control. The consequences of AI will depend on whether legal systems treat it as an unchecked efficiency tool or as a regulated instrument subordinate to legality, rights, and justice.

5. Governance, Regulation, and Legal Reform in the Age of AI Criminal Justice

The governance of artificial intelligence in criminal justice requires a comprehensive legal framework that addresses design, deployment, oversight, liability, transparency, auditability, and remedies. Existing criminal law doctrines are important but insufficient because AI creates risks before harm occurs, during system deployment, and after decisions are made. Regulation must therefore operate across the AI life cycle. It should govern data collection, model training, validation, procurement, institutional use, monitoring, correction, and accountability. Legal regulation in the field of AI has increasingly been discussed as a matter of assessment and future prospects, especially because fragmented legal responses may leave accountability gaps (Zhaltyrbayeva et al., 2023). In criminal justice, fragmentation is particularly dangerous because multiple institutions may rely on AI without common standards. Police agencies, courts, prosecutors, prisons, and private vendors may each apply different rules unless a coherent regulatory structure is established. Such a structure must be grounded in legality, proportionality, transparency, non-discrimination, and human oversight.

Human oversight should be the foundation of AI governance in criminal justice. AI may assist decision-making, but it should not displace legally responsible human actors. The requirement of human oversight is especially important where AI affects liberty, detention, sentencing, surveillance, or criminal suspicion. The EU-oriented discussion of AI in criminal matters emphasizes that technological use must preserve the essence of fundamental rights (Ivan & Manea, 2022). This requires more than a human signature on an automated recommendation. Human oversight must be meaningful, informed, and capable of rejecting AI outputs. Judges, prosecutors, police officers, and prison officials should not treat AI outputs as presumptively correct simply because they are generated by complex systems. Oversight also requires training, documentation, and institutional procedures that allow human decision-makers to understand the limitations of AI. Without meaningful oversight, AI may create a false appearance of human control while effectively transferring decision-making power to machines and private vendors.

Transparency and explainability must also be central regulatory principles. Criminal justice decisions must be open to challenge, and this is impossible if AI systems are secret, proprietary, or technically incomprehensible. AI governance therefore requires documentation obligations, disclosure rules, independent testing, and access mechanisms for affected persons. Transparency and accountability in AI systems have been described as safeguards for well-being in the age of algorithmic decision-making (Cheong, 2024). In criminal justice, these safeguards should include disclosure when AI is used, explanation of how outputs were generated, information about error rates, and access to relevant validation materials. Proprietary secrecy

should not override the right to a fair trial. If a vendor refuses to disclose essential information, courts should be cautious about admitting or relying on the system's outputs. The law must ensure that technological complexity does not become a barrier to defense rights.

Anti-discrimination rules must be integrated into AI governance. Algorithmic discrimination can arise even without explicit discriminatory intent, because models may rely on proxy variables, biased datasets, or historically unequal enforcement patterns. Regulatory measures must therefore require bias testing, impact assessment, continuous monitoring, and corrective obligations. Analysis of algorithmic discrimination, especially in relation to United States legal practices, shows that discrimination can take multiple forms and requires targeted regulatory responses (Wang et al., 2024). In criminal justice, bias assessments should not be optional. AI systems used for policing, bail, sentencing, parole, or surveillance should be evaluated for disparate impact before deployment and periodically afterward. Where discriminatory effects cannot be corrected, the system should not be used. Criminal justice institutions must also avoid the mistake of treating statistical accuracy as sufficient. A system may be accurate in aggregate while still unfair to specific groups or individuals.

Corporate governance is another essential component of AI regulation. Many AI systems used in criminal justice are developed and maintained by private companies. Boards and corporate leaders must therefore understand AI compliance, risk management, liability exposure, and ethical duties. AI governance at the board level has been framed as requiring essential questions about compliance, accountability, and organizational responsibility (Wood, 2024). In the criminal justice context, companies should be required to document design choices, conduct safety testing, disclose limitations, provide audit access, and maintain mechanisms for post-deployment monitoring. Corporate criminal responsibility should apply where companies knowingly or recklessly market unsafe systems, conceal defects, or fail to address foreseeable harms. Compliance programs must be substantive rather than symbolic. The mere existence of an AI ethics statement should not shield a company from liability if its actual practices create unacceptable risks.

Regulation must also address cybersecurity and criminal misuse. AI tools can be exploited for fraud, identity theft, automated hacking, deepfake extortion, and other offenses. Legal frameworks should therefore criminalize intentional harmful use while preserving legitimate research, security testing, and innovation. The relationship between anti-fraud laws and computer science research shows that overly broad criminal provisions can unintentionally obstruct beneficial research that identifies vulnerabilities and improves digital security (Xiao et al., 2025). This is particularly important because AI accountability often depends on external researchers, journalists, civil society organizations, and independent auditors. If legal rules punish good-faith testing, harmful AI systems may remain unexamined. A balanced framework should distinguish malicious exploitation from responsible research and should create safe channels for vulnerability disclosure, algorithmic auditing, and public-interest investigation.

The regulation of autonomous weapons systems requires special attention because the consequences involve life, death, and international criminal responsibility. Autonomous weapons controlled by AI raise legal questions about command responsibility, targeting, distinction, proportionality, and accountability for unlawful harm (Acquaviva, 2022). International legal analysis of autonomous weapon systems emphasizes the need for meaningful human control and compliance with the law of armed conflict (Akkuş, 2022). The criminal justice implications are broader than military law because autonomous weapons illustrate the extreme form of delegating coercive force to machines. If criminal justice systems permit AI to make or strongly determine coercive decisions, they risk replicating similar accountability problems. The principle should be clear: the more serious the consequence, the stronger the requirement of human control, explainability, and legal accountability.

Comparative legal development can provide useful models but also demonstrates regulatory uncertainty. French law has begun addressing AI within broader digital legal reforms, reflecting national attempts to adapt law to technological transformation (Duflot, 2024). Ukrainian criminal law scholarship has examined AI through traditional criminal law categories, showing that legal systems must reinterpret established doctrines in light of new technological realities (Karchevskyi & Radutniy, 2023). International and comparative discussions show that no single model has fully resolved the AI liability problem. Some systems focus on risk regulation, others emphasize data protection, others develop sector-specific rules, and others rely on existing criminal and civil doctrines. For criminal justice, the best approach is likely a hybrid model that combines general AI regulation with specific criminal procedure safeguards, liability rules, professional standards, and institutional oversight.

Ethics should inform regulation but must not replace enforceable legal duties. AI ethics identifies principles such as fairness, accountability, transparency, privacy, and non-maleficence (Mensah, 2024). However, ethical principles can remain vague unless translated into concrete legal obligations. Criminal justice systems require enforceable standards: when AI may be used, who may authorize it, what documentation is required, how outputs may be challenged, what audits are necessary, and what remedies are available for harm. Ethical analysis of AI also shows that technology must be evaluated in relation to human values and social consequences (Stahl, 2021). Therefore, legal reform should connect ethical principles to procedural rules, liability standards, procurement policies, and sanctions. AI ethics should become operational through law, not remain a voluntary language of institutional legitimacy.

Professional education and institutional capacity are also necessary. Judges, prosecutors, lawyers, police officers, and correctional officials need sufficient understanding of AI to evaluate its outputs critically. The work of lawyers in light of AI guidelines suggests that legal professionals must adapt to technological tools while maintaining professional independence and responsibility (Świerczyński, 2021). In criminal justice, this means defense lawyers must be able to challenge algorithmic evidence, prosecutors must disclose AI-assisted methods, judges must scrutinize reliability, and police must understand the limits of predictive tools. Without technical literacy, legal actors may either overtrust AI or reject useful technologies without proper analysis. Regulation should therefore include training requirements, interdisciplinary expert support, and specialized judicial protocols for AI-related evidence and decision-making.

Finally, AI governance must include remedies. A right without a remedy is ineffective, and this is especially true where AI causes criminal justice harm. Individuals affected by AI-based decisions should have access to explanation, correction, appeal, exclusion of unreliable evidence, compensation where appropriate, and institutional review. Responsibility gaps should be addressed through clear duties assigned to developers, vendors, public agencies, and decision-makers (Sio & Mecacci, 2021). Corporate misconduct should be addressed through criminal, administrative, and civil mechanisms where organizational negligence or reckless deployment causes harm (Diamantis, 2021). Public institutions should be accountable for unlawful reliance on AI, and courts should retain authority to reject opaque or discriminatory systems. Legal reform should therefore pursue a human-centered model in which AI is permitted only when it strengthens justice, respects rights, and remains subject to legal control.

6. Conclusion

Artificial intelligence has introduced one of the most profound contemporary challenges to the criminal justice system. Its importance does not lie only in the emergence of new technologies but in the way these technologies transform the basic concepts through which criminal law understands action, responsibility, causation, evidence, judgment, and punishment. Criminal law was historically constructed around human conduct and human blameworthiness. Artificial intelligence, by contrast, operates through data, algorithms, probabilistic outputs, autonomous processing, and complex interactions between human and machine actors. This creates a structural tension between the traditional architecture of criminal responsibility and the technical architecture of intelligent systems. The central conclusion of this study is that criminal justice cannot ignore artificial intelligence, but it also cannot absorb it uncritically. AI must be governed as a powerful legal and social instrument whose use requires strict accountability, transparency, human oversight, and rights protection.

The analysis shows that direct criminal liability of AI remains conceptually and normatively problematic. Criminal punishment presupposes capacities that artificial systems do not possess in the human sense, including moral understanding, blameworthiness, consciousness, and responsiveness to condemnation. Treating AI as a criminal offender risks creating a legal fiction that may obscure the responsibility of developers, users, corporations, public authorities, and institutional decision-makers. The more appropriate approach is to construct a layered model of responsibility. Developers may be responsible for unsafe design, biased data, inadequate testing, or foreseeable misuse. Users and operators may be responsible for intentional misuse, reckless reliance, or negligent supervision. Corporations may be responsible for organizational misconduct, defective compliance systems, or commercial deployment of unsafe technologies. Public institutions may be responsible when they adopt AI systems without sufficient safeguards or allow algorithmic outputs to replace legally accountable human judgment.

The consequences of AI in criminal justice are ambivalent. AI can improve efficiency, support investigation, assist digital forensics, detect cybercrime, organize complex evidence, and help institutions respond to technologically sophisticated

offenses. These benefits are real and should not be dismissed. At the same time, AI can produce algorithmic discrimination, opacity, privacy violations, wrongful suspicion, unjustified detention, unfair sentencing, and institutional overreliance on automated outputs. In criminal justice, even small errors may have severe consequences because the system deals with liberty, dignity, punishment, and state coercion. Therefore, the legitimacy of AI use cannot be measured only by technical accuracy or administrative efficiency. It must be measured by legality, fairness, explainability, equality, proportionality, and the ability of affected persons to challenge decisions.

The article also demonstrates that AI governance must be life-cycle based. Regulation should begin before deployment and continue throughout the system's use. Data collection, training, validation, procurement, deployment, monitoring, auditing, and correction must all be subject to legal standards. Criminal justice institutions should not use AI tools whose logic, data, error rates, or discriminatory effects cannot be meaningfully examined. Proprietary secrecy must not defeat due process. Human oversight must be real, not ceremonial. A human decision-maker must understand the AI system sufficiently to accept, reject, or modify its output. The more severe the legal consequence, the stricter the requirements of explanation, review, and accountability must be.

The future of AI and criminal justice should be built around a human-centered model of technological governance. AI should serve justice rather than redefine justice according to computational convenience. It should assist legal reasoning without replacing judicial responsibility. It should improve investigation without normalizing mass surveillance. It should support crime prevention without weakening the presumption of innocence. It should strengthen institutional capacity without deepening inequality. This requires lawmakers, courts, regulators, companies, and criminal justice professionals to develop clear standards for lawful AI use. The criminal justice system must preserve its normative foundations while adapting its doctrines to technological reality. In this balance between innovation and legality, the guiding principle must remain clear: no artificial system should be allowed to weaken human accountability, fundamental rights, or the moral integrity of criminal justice.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Abbott, R., & Sarch, A. (2024). Punishing Artificial Intelligence: Legal Fiction or Science Fiction. 83-115. https://doi.org/10.1007/978-3-031-47946-5_6

Acquaviva, G. (2022). Autonomous Weapons Systems Controlled by Artificial Intelligence: A Conceptual Roadmap for International Criminal Responsibility. *The Military Law and the Law of War Review*, *60*(1). https://doi.org/10.4337/mllwr.2022.01.06

Akkuş, B. (2022). Autonomous Weapon Systems Under International Law. *Güvenlik Bilimleri Dergisi*, *11*(2), 333-366. https://doi.org/10.28956/gbd.1078155

BĂDescu, V.-S. (2023). Right Today – Between Old Issues and New Challenges or About Justice in a Digital World. *Eblj*, *1*(1). https://doi.org/10.24818/eblj/2022/1/1.03

Chatterjee, S., & N.S, S. (2021). Artificial Intelligence and Human Rights: A Comprehensive Study From Indian Legal and Policy Perspective. *International Journal of Law and Management*, *64*(1), 110-134. https://doi.org/10.1108/ijlma-02-2021-0049

Chaturvedi, M. A., & Tiwari, R. (2023). Cybersecurity in the Age of Artificial Intelligence – Who Should Be Culpable? *Journal of Advanced Zoology*, *44*(S-5), 1478-1483. https://doi.org/10.17762/jaz.v44is-5.1290

Cheong, B. C. (2024). Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-Making. *Frontiers in Human Dynamics*, *6*. https://doi.org/10.3389/fhumd.2024.1421273

Diamantis, M. (2021). Algorithmic Harms as Corporate Misconduct. 135-164. https://doi.org/10.47907/livro2021_4c6

Duflot, A. (2024). Artificial Intelligence in the French Law of 2024. *Legal Issues in the Digital Age*, *5*(1), 37-56. https://doi.org/10.17323/2713-2749.2024.1.37.56
Giannini, A., & Kwik, J. (2023). Negligence Failures and Negligence Fixes. A Comparative Analysis of Criminal Regulation of AI and Autonomous Vehicles. *Criminal Law Forum*, *34*(1), 43-85. https://doi.org/10.1007/s10609-023-09451-1
Ivan, D., & Manea, T. (2022). AI Use in Criminal Matters as Permitted Under EU Law and as Needed to Safeguard the Essence of Fundamental Rights. *International Journal of Law in Changing World*, *1*(1), 17-32. https://doi.org/10.54934/ijlcw.v1i1.15
Karchevskyi, M. V., & Radutniy, O. (2023). Artificial Intelligence in Ukrainian Traditional Categories of Criminal Law. *Herald of the Association of Criminal Law of Ukraine*, *1*(19), 1-25. https://doi.org/10.21564/2311-9640.2023.19.281123
Karnouskos, S. (2021). Symbiosis With Artificial Intelligence via the Prism of Law, Robots, and Society. *Artificial Intelligence and Law*, *30*(1), 93-115. https://doi.org/10.1007/s10506-021-09289-1
Losavio, M. (2021). Algorithms of Machines and Law. *Public Governance Administration and Finances Law Review*, *6*(2), 21-34. https://doi.org/10.53116/pgaflr.2021.2.3
Mensah, G. (2024). AI Ethics. *Ajfra*. https://doi.org/10.62839/ajfra/2024.v1.i1.32-45
Muthukuda Arachchige Dona Shiroma Jeeva Shirajanie, N. (2024). Artificial Intelligence and Sentencing Practices: Challenges and Opportunities for Fairness and Justice in the Criminal Justice System in Sri Lanka. *International Annals of Criminology*, *62*(3-4), 492-542. https://doi.org/10.1017/cri.2024.24
Ness, S., Singh, N., Volkivskyi, M., & Phia, W. J. (2024). The Application of AI and Computer Science in the Context of International Law and Governance "Opportunities and Challenges". *American Journal of Computing and Engineering*, *7*(1), 26-36. https://doi.org/10.47672/ajce.1878
Piparo, C. (2023). Criminal Liability Models and Criminal Participation in the Digital Environment: A Modern Challenge in the Perspective of Italian Constitutionalism. *Zbornik Radova Pravnog Fakulteta Novi Sad*, *57*(4), 1357-1378. https://doi.org/10.5937/zrpfns57-47113
Rodrigues, A., Sousa, S., Algoritmos, Arner, D. W., Barberis, J., Buckley, R. P., Maia, P. I. S., De, A., Martins, S., Ricardo, J., Ramos, M. A., & Roberts, J. (2021). Artificial Intelligence in the Economic Sector: Prevent and Account. https://doi.org/10.47907/livro2021_4
Rodrigues, A. M. (2021). The Last Cocktail - Economic and Financial Crime, Corporate Criminal Responsibility, Compliance and Artificial Intelligence. 119-133. https://doi.org/10.47907/livro2021_4c5
Romero, R. A., & Young, S. D. (2021). Public Perceptions and Implementation Considerations on the Use of Artificial Intelligence in Health. *Journal of Evaluation in Clinical Practice*, *28*(1), 75-78. https://doi.org/10.1111/jep.13580
S, C. G., Shastry, K. A., & A, M. S. M. (2024). Establishing Legal Frameworks to Address Criminal Misuse of AI. *Interantional Journal of Scientific Research in Engineering and Management*, *08*(12), 1-4. https://doi.org/10.55041/ijsrem39392
Sio, F. S. d., & Mecacci, G. (2021). Four Responsibility Gaps With Artificial Intelligence: Why They Matter and How to Address Them. *Philosophy & Technology*, *34*(4), 1057-1084. https://doi.org/10.1007/s13347-021-00450-x
Sitiris, M., & Busari, S. A. (2024). The Legal Capacity (Al-Ahliyyah) of Artificial Intelligence From an Islamic Jurisprudential Perspective. *Malaysian Journal of Syariah and Law*, *12*(1), 31-42. https://doi.org/10.33102/mjsl.vol12no1.453
Stahl, B. C. (2021). Ethical Issues of AI. 35-53. https://doi.org/10.1007/978-3-030-69978-9_4
Swart, M. (2023). Constructing "Electronic Liability" for International Crimes: Transcending the Individual in International Criminal Law. *German Law Journal*, *24*(3), 589-602. https://doi.org/10.1017/glj.2023.28
Świerczyński, M. (2021). AI and the Work of Lawyers in the Light of the Council of Europe Guidelines. 335-346. https://doi.org/10.5771/9783748922834-335
Talukder, K. A., & Shompa, T. F. (2024). Artificial Intelligence in Criminal Justice Management: A Systematic Literature Review. *NHJ*, *1*(01), 63-82. https://doi.org/10.70008/jmldeds.v1i01.42
Velasco, C. (2022). Cybercrime and Artificial Intelligence. An Overview of the Work of International Organizations on Criminal Justice and the International Applicable Instruments. *Era Forum*, *23*(1), 109-126. https://doi.org/10.1007/s12027-022-00702-z
Wang, X., Wu, Y. C., Ji, X., & Fu, H. (2024). Algorithmic Discrimination: Examining Its Types and Regulatory Measures With Emphasis on US Legal Practices. *Frontiers in Artificial Intelligence*, *7*. https://doi.org/10.3389/frai.2024.1320277
Wood, J. M. (2024). AI Governance Check: Navigating Compliance and Essential Queries for Board Discussions. *Board Leadership*, *2024*(194), 1-8. https://doi.org/10.1002/bl.30265
Xiao, M., Sellars, A., & Scheffler, S. (2025). When Anti-Fraud Laws Become a Barrier to Computer Science Research. 1-16. https://doi.org/10.1145/3709025.3712206
Zhaltyrbayeva, R., Tlembayeva, Z., Kurmanova, A. K., Ismailova, B. S., & Smagulova, A. (2023). Legal Regulation in the Field of Artificial Intelligence: Assessment and Prospects. *Journal of Law and Sustainable Development*, *11*(12), e2049. https://doi.org/10.55908/sdgs.v11i12.2049