

The Legislative and Regulatory Framework of Artificial Intelligence Technologies

الإطار التشريعي والتنظيمي لتقنيات الذكاء الاصطناعي

في القانون الجنائي الواقع والآفاق والتحديات

Djokhdem Mohammed*, University of Mansoura (Egypt)

dmsdbws@gmail.com

Received: 01/04 /2026

Accepted: 02/05/2026

Published: 31/05 /2026

Abstract

This study examines the legislative and regulatory framework governing artificial intelligence technologies in criminal law through a critical comparative approach, surveying international and regional legislative experiences and their future prospects. It addresses issues of criminal liability for autonomous AI systems, the inadequacy of traditional criminal statutes to deal with AI-assisted offences, and challenges in digital forensic evidence. A dedicated section maps the applied reality of these technologies within criminal justice systems, analyses future challenges, and explores legislative development prospects. The study concludes that the widening gap between technological reality and existing legal frameworks threatens the principles of criminal justice, necessitating specialised legislation aligned with international human rights standards.

Keywords: Artificial Intelligence, Criminal Law, Criminal Liability, Digital Legislation, Digital Evidence, Regulatory Prospects, Legislative Challenges.

Introduction

Artificial intelligence today represents a multidimensional technological, legal, and social phenomenon, as its applications have permeated all spheres of life, including the criminal justice system. However, this accelerating development poses unprecedented challenges to traditional legislative frameworks built on the principle of natural personhood as the bearer of legal duties, making appropriate legislative grounding a civilizational necessity that cannot be deferred.

Research Problem:

The central research problem revolves around the following question: To what extent do current criminal laws provide a comprehensive and adequate response to the challenges posed by artificial intelligence technologies in the realm of crime, punishment, and liability? What is the actual state of AI deployment in criminal justice systems? And what are the future prospects for its development in light of existing legal and ethical challenges?

Significance of the Study:

The significance of this topic stems from the fact that AI technologies have become a double-edged sword: a tool in the hands of judicial and security authorities to combat and predict crime, while simultaneously a means exploited by criminals to commit highly serious offences ranging from digital fraud and cyberterrorism to evidence forgery and manipulation of judicial systems.

Methodology:

The study employs a critical analytical methodology for examining legal texts, a comparative methodology for evaluating legislative experiences, and a prospective methodology for identifying future challenges and prospects.

* Corresponding Author

This study is divided into five main sections: the first addresses definitional and foundational issues; the second examines the comparative legislative framework; the third is dedicated to criminal liability; the fourth studies the judicial use of AI; and the fifth surveys reality, prospects, and challenges.

Section I: Definitional and Foundational Issues

1.1 Defining Artificial Intelligence in the Criminal Legal Context

There is no unified legal definition of artificial intelligence at the international level, and this conceptual ambiguity itself constitutes an obstacle to drafting effective criminal legislation. The 2024 EU AI Act defines it as an automated system designed to operate with varying degrees of autonomy, generating outputs such as predictions, recommendations, and decisions that affect physical or virtual environments.

Legal scholarship distinguishes three generations of AI with implications for determining liability: the first generation, programmed with fixed rules; the second, based on machine learning that acquires new patterns from data; and the third, based on deep learning, which exhibits behaviours that may exceed what its designers programmed—a development that exacerbates problems of legal attribution (Russell & Norvig, 2021; Al-Shahrani, 2023).

1.2 Characteristics of AI Affecting the Criminal Justice System

AI systems possess characteristics that complicate legislative adaptation in criminal law, most notably: autonomous decision-making, opacity known as the black-box phenomenon, cross-border nature, infinite replicability, and a pace of technological development that permanently outstrips legislative processes.

The Venice Commission's 2023 report identified six criteria that should be considered in any AI regulatory legislation: accountability, transparency, non-discrimination, protection from surveillance, guaranteeing the right to due process, and proportionality between objectives and means (Venice Commission, 2023).

1.3 Challenges of Legal Sovereignty Against Cross-Border AI

The principle of territoriality is one of the most prominent principles of international criminal law, yet AI technologies undermine it by their inherently extra-territorial nature. An algorithm designed in the United States, operated through European servers, and causing harm in the Gulf region raises fundamental questions about jurisdiction and applicable law.

This prompted the European legislator to adopt the principle of extended territorial effect under the General Data Protection Regulation (GDPR), whose provisions apply to any processing of data belonging to EU residents regardless of the processor's location—an approach subsequently incorporated into the 2024 AI Act (Regulation (EU) 2016/679; Al-Ansari, 2022).

Section II: The Comparative Legislative Framework

2.1 The European Experience — The AI Act 2024

The EU AI Act, enacted in April 2024, is the world's first comprehensive legislation regulating these technologies. The Act adopts a risk classification approach with four levels: acceptable, limited, high, and prohibited. Crime and criminal justice are categorised as high-risk applications subject to stringent oversight.

The Act explicitly prohibits several criminal justice applications deemed violations of human rights, most notably: biometric registration systems in public spaces except in exceptional cases, crime prediction applications based on personal characteristics, and emotion recognition systems in interrogation contexts. Fines reach up to 35 million euros or 7% of global sales, whichever is higher (Regulation (EU) 2024/1689; Veale & Zuiderveen Borgesius, 2021).

2.2 The American Experience — The Sectoral Approach

The United States adopts a sectoral approach to AI regulation, distributing responsibilities among multiple federal agencies. In criminal law, the Computer Fraud and Abuse Act of 1986 constitutes the primary basis for prosecuting crimes committed through AI systems.

President Biden issued Executive Order 14110 in 2023, tasking the Department of Justice with preparing guidelines on the use of AI systems in law enforcement and ensuring their constitutional conformity. Under the Trump administration, some of these regulations were relaxed under the banner of encouraging innovation, creating a state of legislative uncertainty (White House, 2023; Engstrom et al., 2020).

2.3 Arab and Gulf Experiences

The United Arab Emirates leads the Arab regulatory landscape with the enactment of Dubai's AI Law in 2024, which establishes a governance framework encompassing transparency and accountability requirements in governmental applications, including judicial ones. Federal Cybercrime Law No. 34 of 2021 also includes provisions criminalising unlawful use of AI tools. Saudi Arabia enacted the Personal Data Protection Regulation in 2021 under Vision 2030. Algeria continues to rely on Law 09/04 relating to cybercrime, with a trend towards comprehensive modernisation. Morocco has initiated the AI Bill 2024, drawing inspiration from the European risk-classification approach (Saudi Royal Decree No. M/19, 2021; Al-Ghamdi, 2024).

Section III: Criminal Liability Arising from AI Use

3.1 The Problem of Criminal Attribution Under Algorithmic Autonomy

Criminal attribution is among the most complex issues generated by AI, as criminal liability traditionally rests on two elements: the material element, embodied in criminal conduct, and the mental element, represented by intent. Highly autonomous AI systems make proving the mental element with respect to natural persons an enormously complex matter.

Legal scholarship proposes three liability models: the vicarious liability model based on solidarity among developer, manufacturer, and user; the distributed liability model according to the degree-of-control criterion; and the independent legal entity model, which advocates granting intelligent systems limited legal personality—an opinion held by a minority of jurists (Hallevy, 2013; Dremljuga et al., 2019).

3.2 Crimes Committed Through Artificial Intelligence

Researchers have documented a range of crimes increasingly committed through AI systems. Foremost are forgery and digital fraud crimes, such as deepfake crimes that use generative technology to produce forged audio or visual content of real individuals for defamation or extortion.

Also prominent are electronic intrusion crimes carried out by AI systems capable of discovering security vulnerabilities and executing sophisticated attacks without direct human guidance, and algorithmic discrimination crimes resulting from systems used in criminal decision-making that produce discriminatory outcomes—a phenomenon extensively documented regarding the COMPAS algorithm in the American justice system (Bou Salem, 2023; Brundage et al., 2018).

3.3 Towards a Renewed Criminal Theory

Some scholars argue that addressing liability problems does not require inventing entirely new concepts, but rather reinterpreting existing ones. The concept of indirect perpetration can be expanded to include those who deploy an intelligent system to commit a crime even if they did not anticipate the specific outcome. Others call for the creation of a specific offence criminalising gross negligence in designing or deploying dangerous AI systems.

Some researchers propose establishing collective compensation funds modelled on nuclear or medical damage funds to compensate for harms caused by AI systems in cases where the

criminally responsible party cannot be definitively identified (Chagal-Feferkorn, 2018; Maghbghab, 2021).

Section IV: Judicial Use of AI Technologies and Its Challenges

4.1 AI in Digital Forensic Evidence

Criminal justice systems in numerous countries have employed AI technologies in the area of evidence, most notably: facial recognition systems for identifying suspects from surveillance cameras, voice and speech analysis systems, and digital forensic tools. However, these tools raise fundamental issues regarding the reliability of extracted evidence and the extent to which it can be contested.

Several American courts have rejected evidence extracted from AI systems due to their failure to meet the required reliability standard under the Daubert standard for accepting scientific evidence, given that the underlying algorithms are not susceptible to independent examination and testing (Daubert v. Merrell Dow Pharmaceuticals, Inc., 1993; Al-Za'bi, 2020).

4.2 Predictive Algorithms and the Right to a Fair Trial

Many countries use criminal prediction systems at various stages of criminal proceedings. These systems calculate the probability of an individual committing a future offence or the likelihood of recidivism, which raises profound concerns from the perspective of the presumption of innocence and the principle of individual criminal responsibility.

The European Court of Human Rights addressed this issue in *Lekic v. Slovenia* (2019), affirming that the use of algorithms in judicial decisions does not relieve courts of their obligation to provide adequate and contestable reasoning. Empirical studies have further demonstrated that algorithms such as COMPAS exhibit bias against African-American individuals in objectively comparable circumstances (Angwin et al., 2016; Dressel & Farid, 2018; Al-Haddad, 2022).

4.3 The Right to Challenge Algorithmic Decisions

The right to defence guarantees access to evidence and the ability to refute it; however, the algorithmic nature of tools protected by intellectual property rights constrains this right. The European legislator addressed this tension in the AI Act by enshrining individuals' right to an explanation of automated decisions affecting them, complementing Article 22 of the GDPR.

In this context, the Wisconsin Supreme Court issued a controversial ruling in *State v. Loomis* (2016), upholding the use of the COMPAS algorithm in sentencing despite the convicted person's refusal to disclose how it works, under the pretext of protecting trade secrets (Wachter et al., 2017).

Section V: Reality, Prospects, and Challenges

5.1 The State of AI Application in Criminal Justice Systems

5.1.1 Actual Applications Worldwide

A survey of contemporary practice reveals the widespread deployment of AI applications across all stages of criminal proceedings. In detection and investigation, the FBI and New York Police Department rely on facial recognition systems, while British police employ crime pattern analysis software to predict geographic hotspots. At the adjudication stage, courts in several American states use the COMPAS algorithm for sentencing recommendations, and European administrative courts use systems to classify and prioritise appeals.

In the Arab context, the UAE leads the field as Dubai's Smart Courts employ a comprehensive AI system to manage case files and schedule hearings, while the Roads and Transport Authority uses a system for analysing accident images and determining liability. In Algeria, security agencies are expanding their use of smart surveillance systems in public spaces without an accompanying clear legislative framework (Dubai Courts, 2023; Ben Houili, 2024).

5.1.2 Findings of Evaluative Studies

Evaluative studies have revealed mixed results. On the positive side, a 2023 study by the US Department of Justice found that the use of geographic crime prediction systems contributed to reducing crime rates by between 10% and 20% in some cities. On the problematic side, an MIT study in 2022 found that error rates in facial recognition systems for dark-skinned individuals reached 34% compared to 0.8% for light-skinned individuals.

The real legal consequences of this reality manifested in a series of lawsuits, most notably the Robert Williams case in Detroit in 2020, who was arrested based on a faulty AI identification, prompting several American cities to issue partial or complete bans on facial recognition technology (Hill, 2020; MIT Media Lab, 2022).

5.2 Prospects for Legislative and Judicial Development

5.2.1 International and Regional Legislative Prospects

At the international level, a multilateral regulatory framework is taking shape. The United Nations launched an international framework convention on AI in September 2024, incorporating principles of governance, accountability, and human rights. The OECD is working to develop binding international standards for regulating AI applications in criminal justice.

At the Arab regional level, the Arab League is moving towards drafting an Arab convention on combating AI-committed cybercrimes, while the GCC General Secretariat is working to unify regulatory frameworks among member states with respect to security and justice applications (UN General Assembly, 2024; Ismail, 2024).

5.2.2 Prospects for Legislatively Supported Technical Development

Legal and technical research is converging on several promising directions, most notably: developing Explainable AI (XAI) that enables judges and lawyers to understand how algorithms reach their decisions; developing independent algorithmic audit tools under the supervision of independent judicial bodies; and developing fair data training protocols to avoid racial and gender biases.

Explainable AI (XAI) is among the most promising technical-legal prospects, as this approach enables judicial parties to access the algorithm's reasoning process step by step, transforming it from a closed black box into a transparent system susceptible to challenge and review.

5.2.3 Prospects for International Judicial Cooperation

The importance of developing international cooperation mechanisms in the area of AI-committed crimes is immense, given their cross-border nature. This can be achieved through expanding the Budapest Protocol on Cybercrime to explicitly include AI crimes, developing mechanisms for exchanging digitally extracted evidence, and establishing an international network of specialised digital forensic laboratories.

Within the G7 framework, the Hiroshima AI Process was launched in 2024, aimed at establishing common principles for AI regulation that include criminal justice aspects—a development representing a promising nucleus for the formation of a comprehensive international system (G7 Hiroshima Summit, 2023; OECD, 2024).

5.3 Legal, Ethical, and Technical Challenges

5.3.1 Structural Legal Challenges

Legislative systems face deep structural challenges in confronting AI, foremost among which is what is known as the legislative time gap—the temporal chasm between the pace of accelerating technological development and the inherently slow pace of legislation. Laws that may take years to prepare may be technologically superseded by the time they are enacted.

There is also the challenge of conflicting interests between driving innovation and preserving fair trial guarantees. Major technology companies frequently oppose any legislation requiring them to disclose their algorithms, citing trade secrets and intellectual property protection—a position that conflicts with the defendant's right to verify digital evidence presented against them.

Added to this are the challenge of fragmented jurisdiction in cross-border crimes, the absence of internationally agreed legal definitions, and the difficulty of determining the moment of harm in algorithmic crimes of gradual accumulation, such as algorithmic discrimination offences (Floridi et al., 2021; Obeidat, 2023).

5.3.2 Ethical and Human Rights Challenges

AI technologies in the criminal domain pose fundamental ethical challenges, foremost the tension between security effectiveness and individual rights. Smart cameras in public spaces may contribute to crime prevention, yet simultaneously threaten the right to privacy, peaceful assembly, and freedom of expression.

Algorithmic bias constitutes a dual ethical and legal challenge, as algorithms generally reflect the biases present in historical training data, which in turn carry the effects of historical societal discrimination. As a result, these systems reproduce discrimination and cloak it in false scientific objectivity, making it more difficult to challenge.

Serious concerns also arise regarding the presumption of innocence under predictive systems, as these systems fundamentally lead to a probabilistic criminal justice that judges the individual based on what they are likely to do rather than what they have actually done—a position that contradicts the philosophical foundation of individual criminal responsibility (Završnik, 2019; Al-Qadi, 2023).

5.3.3 Technical Challenges with Legal Dimensions

At the technical level, AI systems generate challenges with precise legal dimensions, most notably the problem of performance instability, where the same system may produce different results under similar conditions, undermining the consistency essential to judicial rulings. This is compounded by the problem of Concept Drift—the phenomenon of a model's declining accuracy over time as social patterns change without updates to training data.

Among the most significant technical challenges is the disparity between a system's accuracy in the testing environment and its accuracy in actual application—a discrepancy that strips many of the positive results announced about these systems of much of their credibility and raises serious questions about the reliability of evidence extracted by them for use in criminal verdicts (Roth, 2022; Berk et al., 2021).

5.3.4 Challenges of the Digital Divide Between Nations

The digital divide manifests in the context of criminal AI on two intertwined levels. The first is the technical gap between developed countries capable of developing and deploying these technologies and developing countries that import them without the capacity to audit or adapt them—rendering their judicial systems hostage to technical decisions made by foreign corporations. The second is the legislative gap that makes countries with weaker legislation destinations for the export of algorithmic practices prohibited in more protective countries.

The 2024 UNDP Human Development Report notes that 67% of developing countries lack the qualified human resources to examine and audit AI systems used in their judicial systems—a serious human rights gap requiring urgent international intervention (UNDP, 2024).

5.4 Proposals for a Comprehensive Regulatory Framework

In light of the foregoing analysis of reality, prospects, and challenges, a comprehensive regulatory framework is proposed resting on the following pillars:

Pillar One — Graduated and Adaptive Legislation: Adopting flexible criminal legislation built on the principle of risk-based graduated regulation following the European model, incorporating periodic review mechanisms to keep pace with technological development without the need for complete re-legislation.

Pillar Two — Specialised Supervisory Bodies: Establishing independent bodies specialised in auditing criminal AI systems, comprising legal, technical, and human rights experts, responsible

for accrediting systems, monitoring their performance, and issuing periodic reports on their biases and risks.

Pillar Three — Fair Trial Guarantees: Enshrining the defendant's right to access the workings of algorithms used in their case and to challenge them, and obliging judicial bodies not to rely exclusively on AI outputs in any criminal decision.

Pillar Four — International Cooperation: Joining relevant international instruments and developing protocols for exchanging digital evidence and extradition agreements in AI-committed crimes, with particular attention to strengthening the capacity of developing countries in this area (Council of Europe, 2022; Al-Khalaf, 2024).

Conclusion and Findings

Main Findings

1. The existing criminal legislative framework in most Arab countries suffers from obvious shortcomings in confronting the challenges posed by AI, as most of these countries remain bound by texts originally designed to deal with traditional cybercrime.
2. Applied reality has revealed a stark contradiction between the security effectiveness of these technologies and their documented human rights risks, particularly regarding racial and gender algorithmic bias and the presumption of innocence.
3. The European experience, as represented in the 2024 AI Act, presents an advanced model that can be drawn upon while adapting it to the legal and cultural specificities of Arab systems.
4. The digital divide between nations emerges as a recurring human rights challenge requiring a solidarity-based international response to prevent the export of prohibited algorithmic practices to weaker legal environments.
5. Explainable AI (XAI) is among the most promising prospects for resolving the problem of reconciling the judicial use of these technologies with fair trial guarantees.

Recommendations

1. Expedite the enactment of criminal legislation specialised in AI, incorporating a precise legal definition, a flexible liability system that accounts for the degree of system autonomy, and mechanisms for oversight and control.
2. Establish independent specialised supervisory bodies responsible for certifying criminal AI systems before deployment and ensuring their compliance with human rights and technical standards.
3. Develop clear standards for the admissibility of digital evidence extracted through AI that ensure its genuine susceptibility to challenge and review.
4. Join relevant international instruments and strengthen Arab regional cooperation in the field of criminal AI regulation.
5. Invest in building specialised human resources—judges, lawyers, and investigators—in the field of AI through specialised and ongoing training programmes.

In conclusion, the issue of regulating artificial intelligence in the criminal domain remains the defining justice challenge of the twenty-first century. The legislator who is conscious of the weight of this responsibility does not merely hasten to fill legal voids, but establishes a framework guaranteeing permanent balance between technical effectiveness and human dignity. The speed of the algorithm must never come at the price of the slowness of justice.

References

Arabic Sources (Translated)

- Al-Ansari, M. H. (2022). Digital sovereignty and issues of judicial jurisdiction in cybercrime. *Journal of Sharia and Law, UAE University*, 36(89), 195–240.

- Ismail, R. M. (2024). Towards a unified Arab convention on AI regulation. *International Politics Journal*, Al-Ahram Foundation, 59(238), 112–130.
- Ben Houili, M. (2024). The right to challenge algorithmic decisions in light of comparative legislation. *Journal of Judicial Ijtihad*, Mohamed Khider University Biskra, 16(1), 67–98.
- Bou Salem, A. R. (2023). Cybercrime in light of AI technologies: Towards a comparative criminal foundation. *Journal of Comparative Legal Studies*, University of Constantine 2, 9(17), 112–145.
- Al-Haddad, H. M. (2022). Predictive algorithms and criminal principles: A comparative study. *Journal of Law and Economics*, Cairo University, 92(1), 315–362.
- Al-Khalaf, A. M. (2024). International cooperation in combating cybercrime. *Dar Al-Nahda Al-Arabiya*, Cairo.
- Khalil, I. A. (2024). Towards a fair digital criminal system in the age of algorithms. *Egyptian Journal of Legal and Economic Studies*, 18(2), 67–102.
- Al-Za'bi, K. M. (2020). Digital forensic evidence: Legality and admissibility standards. *Dar Al-Thaqafa*, Amman.
- Al-Shahrani, F. S. (2023). Employing AI technologies in criminal justice. *Journal of Law and Humanities*, Ziane Achour University Djelfa, 16(2), 45–67.
- Obeidat, O. S. (2023). Legal challenges of AI in criminal justice systems. *An-Najah National University Research Journal — Humanities*, 37(4), 891–930.
- Al-Ghamdi, A. M. (2024). Legal regulation of AI in Saudi Arabia in light of Vision 2030. *Journal of Legal and Political Sciences*, Shaqra University, 15(1), 23–58.
- Al-Qadi, A. F. (2023). The presumption of innocence facing algorithmic justice. *Journal of Law and Political Science*, Ain Shams University, 15(3), 241–280.
- Maghbghab, N. (2021). Criminal liability of AI in Lebanese and comparative law. *Lebanese Legal Journal*, 14(2), 77–118.
- Strategic and International Studies Institute. (2023). Artificial intelligence and justice in the Arab world: An assessment report. Emirates Centre for Strategic Studies, Abu Dhabi.
- Saudi Personal Data Protection Regulation. (2021). Royal Decree No. M/19, 1443 AH. Official Gazette, Saudi Arabia.
- Law No. 09-04 of 5 August 2009 on rules for preventing and combating offences related to information and communication technologies. Official Journal, No. 47, People's Democratic Republic of Algeria.

Foreign Sources

- Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias: There's software used across the country to predict future criminals. ProPublica Investigative Report.
- Berk, R., Heidari, H., Jabbari, S., Kearns, M., & Roth, A. (2021). Fairness in criminal justice risk assessments: The state of the art. *Sociological Methods & Research*, 50(1), 3–44. <https://doi.org/10.1177/0049124118782533>
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Future of Humanity Institute, University of Oxford.
- Chagal-Feferkorn, K. (2018). The reasonable algorithm. *Journal of Law, Technology & Policy*, 2018(1), 111–145.
- Council of Europe. (2022). Budapest Convention Additional Protocol. Council of Europe Treaty Series.
- Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).
- Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 4(1), e1701544. <https://doi.org/10.1126/sciadv.aao5580>

- Dremluga, R., Kuznetsov, P., & Mamychyev, A. (2019). Criteria for recognition of AI as a legal entity. *Journal of Politics and Law*, 12(3), 105–111.
- Dubai Courts. (2023). AI integration in judicial processes. Dubai Courts Annual Report. Dubai Courts Publications.
- Engstrom, D. F., Ho, D. E., Sharkey, C. M., & Cuéllar, M. F. (2020). Government by algorithm: Artificial intelligence in federal administrative agencies. Stanford Law School.
- European Parliament and Council. (2016). Regulation (EU) 2016/679 (GDPR), Article 3. *Official Journal of the European Union*, L 119/1.
- European Parliament and Council. (2024). Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act). *Official Journal of the European Union*.
- Floridi, L., Cowls, J., King, T. C., & Taddeo, M. (2021). How to design AI for social good: Seven essential factors. *Science and Engineering Ethics*, 26(3), 1771–1796.
- G7 Hiroshima Summit. (2023). Hiroshima process international guiding principles for advanced AI systems. G7 AI Leaders' Summit.
- Hallevy, G. (2013). When robots kill: Artificial intelligence under criminal law. Northeastern University Press.
- Hill, K. (2020, June 24). Wrongfully accused by an algorithm. *The New York Times*.
- MIT Media Lab. (2022). Gender shades: Intersectional accuracy disparities in commercial gender classification. MIT Publications.
- OECD. (2024). Recommendation of the Council on Artificial Intelligence. OECD Publishing.
- Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press.
- Roth, A. (2022). Machine testimony. *Yale Law Journal*, 133(6), 1972–2040.
- Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
- State v. Loomis, 881 N.W.2d 749 (Wis. 2016).
- UN General Assembly. (2024). Resolution A/78/L.49 — Seizing the opportunities of safe, secure and trustworthy AI systems. United Nations.
- UNDP. (2024). Human development report: AI for human development (pp. 134–156). United Nations Development Programme.
- Veale, M., & Zuiderveen Borgesius, F. (2021). Demystifying the draft EU artificial intelligence act. *Computer Law Review International*, 22(4), 97–112.
- Venice Commission. (2023). Rule of law and artificial intelligence (CDL-AD(2023)034). Council of Europe.
- Wachter, S., Mittelstadt, B., & Russell, C. (2017). Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology*, 31(2), 841–887.
- White House. (2023). Executive Order 14110 on the safe, secure, and trustworthy development and use of artificial intelligence. 88 Fed. Reg. 75191.
- Završnik, A. (2019). Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*, 18(5), 623–642.