ARTIFICIAL INTELLIGENCE AND CRIMINAL LIABILITY: A GLOBAL ANALYSIS OF THE RISKS OF ALGORITHMS IN THE CRIMINAL JUSTICE SYSTEM

Basuki[1], Abdul Latif[2], Supaphorn Akkapin[3]
[12]Doctor of Law Studies Program Postgraduate Program - Jayabaya University-Indonesia
[3]Rajamangala University of Technology Krungthep - Thailand
Email : [1]infobisa17@gmail.com, [2]prof.abdul.latif59@gmail.com,
[3]Supaphorn.k@mail.rmutk.ac.th

Keywords:

First keyword: Artificial Intelligence
Second keyword: Criminal Liability
Third keyword: Algorithm Risk
Fourth keyword: Criminal Justice System
Fifth keyword: Comparative Law

Article History:

Received: 2025-08-30
Accepted: 2025-09-23
Published: 2025-09-30

ABSTRACT

The integration of artificial intelligence (AI) into criminal justice systems has revolutionized decision-making processes but, at the same time, has raised profound legal and ethical issues. This article critically examines the various risks arising from the use of algorithmic systems in the judicial process, particularly with regard to criminal liability. Through a normative-comparative approach to the legal frameworks in the United States, Germany, China, and the European Union, this study identifies structural gaps in the regulation of automated decisions that can lead to harm or injustice. Findings indicate that conventional criminal liability doctrines are inadequate to address the challenges posed by the non-human and autonomous actions of AI systems. In response, this study proposes a hybrid liability framework that combines command responsibility and sociotechnical liability approaches into a new theoretical model aimed at achieving accountability in a digitized legal context. Furthermore, this study encourages international legal harmonization to ensure equal protection, as well as the establishment of global standards for transparency and oversight in the use of algorithms within criminal justice systems. Thus, this article contributes to the development of criminal law that is adaptive to digital realities and algorithmic governance.

1. INTRODUCTION

In recent years, the integration of artificial intelligence (AI) into criminal justice systems has expanded rapidly across multiple countries[1];[2]. This technology is applied in diverse forms, such as software for assessing the risk of recidivism, facial recognition for identifying suspects, and algorithms that support legal decision-making[3];[4]. For example, in the United States, the COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) system has been used by a number of jurisdictions to assist judges in determining bail amounts and sentencing[5];[6]. However, research by ProPublica (2016) indicates that COMPAS exhibits racial bias, with Black defendants more frequently predicted to be at high risk of reoffending than White defendants, despite this not being the case in reality[7];[8].

A similar phenomenon is occurring in China, which is actively developing AI-based surveillance systems through facial recognition

[1] K Blount, "Using Artificial Intelligence to Prevent Crime: Implications for Due Process and Criminal Justice," *AI and Society* 39, no. 1 (n.d.), https://doi.org/10.1007/s00146-022-01513-z.

[2] B Dupont et al., "Artificial Intelligence in the Context of Crime and Criminal Justice," *SSRN Electronic Journal*, n.d., https://doi.org/10.2139/ssrn.3857367.

[3] M Bagaric et al., "The Solution to the Pervasive Bias and Discrimination in the Criminal Justice: Transparent Artificial Intelligence," *American Criminal Law Review* 59, no. 1 (n.d.).

[4] C McKay, "Predicting Risk in Criminal Procedure: Actuarial Tools, Algorithms, AI and Judicial Decision-Making," *Current Issues in Criminal Justice* 32, no. 1 (n.d.), https://doi.org/10.1080/10345329.2019.1658694.

[5] T Brennan and W Dieterich, "Correctional Offender Management Profiles for Alternative Sanctions (COMPAS," in *Handbook of Recidivism Risk/Needs Assessment Tools*, n.d., https://doi.org/10.1002/9781119184256.ch3.

[6] P S Putra and F S Siagian, "The Capability of Artificial Intelligence in Calculating the Losses of Crime Victims," *Kosmik Hukum* 25, no. 2 (n.d.), https://doi.org/10.30595/kosmikhukum.v25i2.25817.

[7] M Hamilton, "The Biased Algorithm: Evidence of Disparate Impact on Hispanics," *American Criminal Law Review* 56, no. 4 (n.d.).

[8] R Karthikeyan, C Yi, and M Boudourides, "Criminal Justice in the Age of AI: Addressing Bias in Predictive Algorithms Used by Courts," in *The Ethics Gap in the Engineering of the Future* (Emerald Publishing Limited, n.d.), 27–50, https://doi.org/10.1108/978-1-83797-635-520241003.

technology and big data to enable early detection of potential crimes[9];[10]. Meanwhile, in Europe, the discourse on Ethical AI continues to evolve alongside the European Union's initiatives to establish a legal framework emphasizing the principles of transparency, accountability, and the avoidance of discrimination[11];[12];[13];[14]. However, the adoption of AI in law enforcement is not necessarily accompanied by a ready legal framework, particularly regarding criminal liability for errors or deviations in algorithmic results that affect individual rights[15];[16].

The urgency of this research lies in the legal vacuum that emerges when decisions affecting a person's fate are significantly influenced by non-human systems—namely, algorithms. In the context of a criminal justice system that upholds the principles of legality, caution, and individual responsibility, the use of AI presents both philosophical and practical challenges. If errors occur that result in harm or violations of human rights, the question arises: Who should be held criminally liable—the software developer, the user institution, or the AI itself? Furthermore, the opacity of algorithmic logic—known as

[9] Z Ahmed Khan and A Rizvi, "AI Based Recognition Technology and Criminal Justice: Issues and Challenges," *Turkish Journal of Computer and Mathematics Education* 12, no. 14 (n.d.).

[10] N Wang and M Y Tian, "Intelligent Justice': AI Implementations in China's Legal Systems," n.d., https://doi.org/10.1007/978-3-030-88615-8_10.

[11] J Laux, S Wachter, and B Mittelstadt, "Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act," *SSRN Electronic Journal*, n.d., https://doi.org/10.2139/ssrn.4365079.

[12] S Musch, M Borrelli, and C Kerrigan, "The EU AI Act: A Comprehensive Regulatory Framework for Ethical AI Development," *SSRN Electronic Journal*, n.d., https://doi.org/10.2139/ssrn.4549248.

[13] N A Smuha et al., "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act," *SSRN Electronic Journal*, n.d., https://doi.org/10.2139/ssrn.3899991.

[14] I Ulnicane, "Artificial Intelligence in the European Union: Policy, Ethics and Regulation," in *The Routledge Handbook of European Integrations*, n.d., https://doi.org/10.4324/9780429262081-19.

[15] A O M Al-Dulaimi and M.A.-A.W. Mohammed, "Legal Responsibility for Errors Caused by Artificial Intelligence (AI) in the Public Sector," *International Journal of Law and Management*, n.d., https://doi.org/10.1108/IJLMA-08-2024-0295.

[16] B Custers, "AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law," *SSRN Electronic Journal*, n.d., https://doi.org/10.2139/ssrn.4331759.

"black-box" AI—exacerbates the difficulty of tracing errors and assigning responsibility[17];[18];[19];[20].

Previous studies have largely focused on the ethical implications of AI use or on analyzing systemic bias in algorithms[21];[22];[23];[24] . However, limited research has directly examined the issue of criminal liability from a comparative, cross-national perspective. This represents a significant research gap, given that AI is already employed in judicial systems across jurisdictions with differing legal approaches. The absence of a conceptual framework linking criminal responsibility to algorithmic decision-making poses serious risks to the protection of defendants' rights, judicial accountability, and overall legal certainty.

Based on this background, this study aims to analyze how algorithmic risks in criminal justice systems are addressed in different countries and to identify relevant forms of criminal liability for AI-based errors. The scientific contribution of this research lies in developing a legal framework that bridges technological innovation with the principles of criminal justice, while promoting the harmonization of criminal norms in an increasingly complex digital era.

---

[17] C Rudin and J Radin, "Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From An Explainable AI Competition," *Harvard Data Science Review* 1, no. 2 (n.d.), https://doi.org/10.1162/99608f92.5a8a3a3d.

[18] C A TSCHIDER, "Beyond the "black Box," *Denver Law Review* 98, no. ue 3) (n.d.), https://doi.org/10.1090/noti1408.

[19] W J Eschenbach, "Transparency and the Black Box Problem: Why We Do Not Trust AI," *Philosophy and Technology* 34, no. 4 (n.d.), https://doi.org/10.1007/s13347-021-00477-0.

[20] T Wischmeyer, "Artificial Intelligence and Transparency: Opening the Black Box," in *Regulating Artificial Intelligence* (Springer International Publishing, n.d.), 75–101, https://doi.org/10.1007/978-3-030-32361-5_4.

[21] N Gupta, "Artificial Intelligence Ethics and Fairness: A Study to Address Bias and Fairness Issues in AI Systems, and the Ethical Implications of AI Applications," *Revista Review Index Journal of Multidisciplinary* 3, no. 2 (n.d.), https://doi.org/10.31305/rrijm2023.v03.n02.004.

[22] N Kordzadeh and M Ghasemaghaei, "Algorithmic Bias: Review, Synthesis, and Future Research Directions," *European Journal of Information Systems* 31, no. ue 3) (n.d.), https://doi.org/10.1080/0960085X.2021.1927212.

[23] E Ntoutsi et al., "Bias in Data-Driven Artificial Intelligence Systems—An Introductory Survey," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 10, no. 3 (n.d.), https://doi.org/10.1002/widm.1356.

[24] J Shuford, "Examining Ethical Aspects of AI: Addressing Bias and Equity in the Discipline," *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023* 3, no. 1 (n.d.): 262–280, https://doi.org/10.60087/jaigs.v3i1.119.

2. RESEARCH OBJECTIVES

This study addresses the urgent need for an adequate legal framework to regulate advances in artificial intelligence (AI) technology that have permeated crucial areas of the criminal justice system. In a global context, the use of AI in legal decision-making not only enhances efficiency but also raises legal issues that have not yet been fully anticipated by national or international legal systems. Accordingly, this study aims to explore, analyze, and formulate normative approaches to addressing questions of criminal liability in cases of algorithmic errors that affect individual rights and freedoms.

Specifically, the study seeks to identify algorithmic risks that could lead to issues within the criminal justice system, including potential bias, discrimination, and harmful prediction errors. It also examines the extent to which positive legal instruments in several jurisdictions—such as the United States, Germany, the European Union, and China—provide protection against the adverse effects of AI, as well as the ways in which criminal liability frameworks can be adapted to address situations involving non-human entities.

Furthermore, this study intends to contribute both theoretically and practically to the development of criminal law that is responsive to technological change. On the theoretical side, it aims to bridge traditional theories of criminal responsibility with emerging concepts in legal technology. On the practical side, the results are expected to serve as a reference for policymakers, law enforcement officials, and technology developers in formulating regulations and ethical guidelines that maintain a balance between technological efficiency and the protection of human rights.

3. RESEARCH METHODOLOGY

This study adopts a normative-comparative legal approach with an emphasis on analyzing positive legal norms and legal instruments that regulate or relate to the use of artificial intelligence in the criminal justice

system[25];[26];[27];[28];[29]. This approach was chosen because the main problem in this study does not lie in empirical facts, but rather in the norms, principles, and legal foundations that must respond to increasingly complex developments in smart technology. The normative approach enables an examination of the structure of relevant legal norms and principles, while the comparative approach facilitates an understanding of regulatory dynamics across countries as a basis for reflection on the development of national and international law.

The data used in this study are secondary data obtained through library research. The sources comprise primary legal documents such as laws, regulations, public policies, and court decisions from selected jurisdictions, namely the United States, Germany, China, and the European Union. Secondary legal sources, including books, scientific journal articles, international agency reports, and relevant academic publications on AI and criminal law, were also consulted. The selection of these countries was based on the variety of legal approaches and the level of AI utilization in their respective judicial systems, which together provide a comprehensive overview of global challenges and regulatory responses.

Data collection was conducted through document review and electronic literature searches in leading scientific databases such as Scopus, ScienceDirect, SpringerLink, and HeinOnline. Data analysis was conducted qualitatively through three main stages: (1) identifying legal norms or principles related to criminal liability for algorithmic actions; (2) classifying legal risks based on forms of algorithmic errors in criminal justice systems;

---

[25] S Amelia, "Progressive Legal Approach to Modern Community Law Enforcement in Indonesia," *Pancasila and Law Review* 4, no. 1 (n.d.), https://doi.org/10.25041/plr.v4i1.2729.

[26] C Aspalter, "From Descriptive to Normative Comparative Social Policy: By Way of Conclusion," in *Ideal Types in Comparative Social Policy*, n.d.

[27] Y Gunawan, "Legal Research Perspective through Problem Solution Approach," *International Journal of Science and Society* 5, no. 2 (n.d.), https://doi.org/10.54783/ijsoc.v5i2.705.

[28] E V Kirdyashova, *Towards an Interdisciplinary Approach in Public Legal Research* (Courier of Kutafin Moscow State Law University (MSAL, n.d.), https://doi.org/10.17803/2311-5998.2023.104.4.041-051.

[29] Moh M Rohman et al., *Methodological Reasoning Finds Law Using Normative Studies (Theory, Approach and Analysis of Legal Materials* (MAQASIDI: Jurnal Syariah Dan Hukum, n.d.), https://doi.org/10.47498/maqasidi.v4i2.3379.

and (3) comparing regulatory approaches and accountability in each jurisdiction.

To maintain the validity and reliability of the data, triangulation of legal sources and cross-referencing of literature were undertaken. Additionally, the researcher employs both deductive and inductive approaches in alternation to interpret normative data and construct a comprehensive legal argument. This methodological design aims to ensure that the research findings are not merely descriptive but also capable of generating normative recommendations that are practically implementable in addressing issues of criminal liability within the context of artificial intelligence.

4. RESULT

4.1 Algorithmic Risk Constellations in the Criminal Justice System

The integration of artificial intelligence (AI) into criminal justice systems has serious implications for the principle of substantive justice[30];[31];[32]. While this technology promises efficiency and objectivity, its implementation, in reality, reveals numerous systemic algorithmic risks[33];[34]. Through a cross-jurisdictional review, three main patterns of risk can be identified: first, algorithmic bias stemming from historical training data[35];[36];[37]

[30] R M Re et al., "Developing Artificially Intelligent Justice," *Stanford Technology Law Review* 22 (n.d.).

[31] A R Vargas-Murillo et al., "Transforming Justice: Implications of Artificial Intelligence in Legal Systems," *Academic Journal of Interdisciplinary Studies* 13, no. 2 (n.d.), https://doi.org/10.36941/ajis-2024-0059.

[32] A Završnik, "Criminal Justice, Artificial Intelligence Systems, and Human Rights," *ERA Forum* 20, no. 4 (n.d.), https://doi.org/10.1007/s12027-020-00602-0.

[33] V Galaz et al., "Artificial Intelligence, Systemic Risks, and Sustainability," *Technology in Society* 67 (n.d.), https://doi.org/10.1016/j.techsoc.2021.101741.

[34] M U Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies," *SSRN Electronic Journal*, n.d., https://doi.org/10.2139/ssrn.2609777.

[35] Abdul Wajid Fazil, Musawer Hakimi, and Amir Kror Shahidzay, "A Comprehensive Review Of Bias In Ai Algorithms," *Nusantara Hasana Journal* 3, no. 8 (n.d.), https://doi.org/10.59003/nhj.v3i8.1052.

[36] Hamilton, "The Biased Algorithm: Evidence of Disparate Impact on Hispanics."

[37] Kordzadeh and Ghasemaghaei, "Algorithmic Bias: Review, Synthesis, and Future Research Directions."

second, lack of transparency in AI-based decision-making processes[38];[39] and third, systemic failure to account for the complexity of the socio-legal context[40];[41];[42]. These three elements collectively threaten fundamental legal principles, such as due process and the presumption of innocence, and exacerbate existing inequalities within the criminal justice system.

As a concrete example, the application of predictive algorithms in the COMPAS system in the United States illustrates how historical bias can be institutionalized through technology[43];[44]. This system, designed to assist in sentencing, was trained using police data that disproportionately targeted Black communities. As a result, COMPAS exhibited a significantly higher false-positive rate for defendants from minority groups. A similar phenomenon occurred in China through a facial recognition system that demonstrated low accuracy for Uyghur citizens, indirectly facilitating ethnic profiling. This situation highlights a critical paradox: rather than improving objectivity, AI technology institutionalizes historical prejudices. This occurs because machine learning models treat biased historical data as "ground truth," thereby reinforcing existing structural discrimination.

In addition to the issue of bias, the opacity of AI decision-making also poses fundamental challenges to the principle of legal transparency. Many AI systems, particularly those using deep learning models, function as "black boxes" that do not provide understandable explanations for their decisions. This opacity directly contradicts the principle of the right to a fair trial, as enshrined in Article 14 of the International Covenant on Civil and Political

---

[38] T Dancy and M Zalnieriute, "AI and Transparency in Judicial Decision-Making," *SSRN Electronic Journal*, n.d., https://doi.org/10.2139/ssrn.5331491.

[39] Wischmeyer, "Artificial Intelligence and Transparency: Opening the Black Box."

[40] M Callier and H Callier, "Blame It on the Machine: A Socio-Legal Analysis of Liability in an Blame It on the Machine: A Socio-Legal Analysis of Liability in an AI World AI World," *Technology & Arts Washington Journal of Law* 14 (n.d.).

[41] H Gaffar, "Implications of Digitalization and AI in the Justice System: A Glance at the Socio-Legal Angle," *Law and World* 10, no. 3 (n.d.): 154–177, https://doi.org/10.36475/10.3.14.

[42] S Larsson, "The Socio-Legal Relevance of Artificial Intelligence," *Droit et Societe* 103, no. 3 (n.d.), https://doi.org/10.3917/drs1.103.0573.

[43] M P B Carbo, "Machine Learning Applications in the United States Criminal Justice System: A Critical Content Analysis of the COMPAS Recidivism Risk Assessment" (Nan, n.d.).

[44] W Gravett, "Sentenced by an Algorithm — Bias and Lack of Accuracy in Risk-Assessment Software in the United States Criminal Justice System," *South African Journal of Criminal Justice* 34, no. 1 (n.d.), https://doi.org/10.47348/sacj/v34/i1a2.

Rights (ICCPR), which requires that defendants be informed of the reasons behind decisions affecting their liberty. For example, if a risk assessment algorithm denies a bail request without a rational explanation, this not only erodes judicial accountability but also risks undermining public trust in the legal system. In this context, experts such as Cynthia Rudin argue that the dichotomy between accuracy and clarity is flawed; however, in practice, many commercially deployed AI systems prioritize technical complexity over ethical transparency, thereby exacerbating the tension between efficiency and justice[45];[46].

Furthermore, AI systems often overlook complex and inherently human socio-legal factors, such as the psychological condition of the defendant, experiences of social marginalization, or local economic-political dynamics. The inability of AI systems to capture these nuances results in "contextual blindness"—the tendency to reduce individuals to statistical profiles. For example, predictive policing algorithms may flag economically disadvantaged neighborhoods as crime-prone simply because historical data reflects high levels of law enforcement in those areas, even when such patterns arise from over-policing practices. Consequently, cycles of surveillance are perpetuated, reinforcing stigma against specific demographic groups. These limitations underscore the incompatibility between the deterministic logic of AI and the discretionary logic of the judiciary, which, in practice, accommodates empathy, mitigating circumstances, and substantive values of justice.

Based on these findings, it can be concluded that the algorithmic risks inherent in the use of AI in the criminal justice system have transformed the role of technology from a mere tool to an active agent of injustice. Therefore, the response to this issue cannot be merely technocratic but must entail structural reforms grounded in the principle of algorithmic accountability. Such reforms should involve four principal pillars: first, bias audits of the training data; second, the mandatory application of explainability standards in AI systems used in the legal field; third, training for judges and legal

[45] A Haim, "The Administrative State and Artificial Intelligence: Toward an Internal Law of Administrative Algorithms," *SSRN Electronic Journal*, n.d., https://doi.org/10.2139/ssrn.4498470.

[46] D Leslie, "Tackling COVID-19 through Responsible AI Innovation: Five Steps in the Right Direction," *SSRN Electronic Journal*, n.d., https://doi.org/10.2139/ssrn.3652970.

officials to critically evaluate algorithmic outputs; and fourth, the establishment of a robust legal framework to determine accountability in the event of errors arising from the use of AI. Without such a foundation, the digitization of the judicial system will not only fail to enhance justice but will instead usher in an era of "automated injustice," in which existing inequalities are reinforced under the illusion of technological neutrality.

4.2 The Unpreparedness of Positive Legal Instruments for Algorithmic Criminal Liability

A crucial finding of this study is the absence of comprehensive criminal liability regimes in all jurisdictions examined to address failures or malfunctions of autonomous AI systems. Existing regulations, such as the EU Artificial Intelligence Act (still in the legislative process), predominantly focus on ex ante aspects, such as risk management, ethical standards, and personal data protection[47];[48];[49]. However, this approach conspicuously overlooks clear ex post mechanisms for establishing criminal liability when AI systems cause concrete harm. In the United States, the current legal framework tends to rely on the concept of vicarious liability[50];[51], whereby government agencies or technology vendors, acting as users or producers, may be held liable in civil or administrative proceedings. Unfortunately, this framework is inherently not designed for—and is highly inadequate in addressing—the criminal liability of individuals or corporations arising specifically from the autonomy and unpredictability of AI systems.

Furthermore, attempts to apply traditional criminal law concepts face fundamental philosophical and practical obstacles. Core doctrines such as mens rea (the element of fault, intent, or negligence) and actus reus (a physical

[47] Laux, Wachter, and Mittelstadt, "Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act."

[48] C Orwat et al., "Normative Challenges of Risk Regulation of Artificial Intelligence and Automated Decision-Making," *SSRN Electronic Journal*, n.d., https://doi.org/10.2139/ssrn.4274828.

[49] U Pagallo, J Ciani Sciolla, and M Durante, "The Environmental Challenges of AI in EU Law: Lessons Learned from the Artificial Intelligence Act (AIA) with Its Drawbacks," *Transforming Government: People, Process and Policy* 16, no. 3 (n.d.), https://doi.org/10.1108/TG-07-2021-0121.

[50] M E Diamantis, "Vicarious Liability for AI," *Indiana Law Journal* 99, no. 1 (n.d.).

[51] D Glavaničová and M Pascucci, "Vicarious Liability: A Solution to a Problem of AI Responsibility?," *Ethics and Information Technology* 24, no. 3 (n.d.), https://doi.org/10.1007/s10676-022-09657-8.

act that is against the law) strictly require a human legal subject with consciousness and will. As a result, AI systems operating autonomously, even through complex decision-making processes, cannot meaningfully be intended to commit crimes or possess consciousness of their actions. This condition creates a legal vacuum in criminal liability, particularly in scenarios where fatal or socially significant harm (e.g., in autonomous weapon systems, automated medical diagnoses, or self-driving vehicles) arises directly from algorithmic decisions without identifiable human intervention at the time of the event. This vacuum not only hinders fair prosecution efforts but also has the potential to weaken the deterrence effect, which is a primary objective of criminal law.

A significant additional challenge arises in approaches that seek to impose criminal liability solely on corporations (as producers or primary users of AI) based on negligence in oversight. This approach faces insurmountable evidentiary hurdles. Establishing a clear and direct causal nexus between the specific actions or omissions of individual humans within a corporation and the harmful outcomes produced by autonomous AI systems is an exceedingly complex task. This is primarily due to the "black box" nature of certain algorithms, the intricate interactions between input data and system outputs, and the potential impossibility of accurately predicting how AI will behave in all real-world scenarios. As a result, the burden of proof that prosecutors must meet in such cases becomes exceedingly burdensome—if not impossible—often rendering criminal prosecution futile.

Recognizing the complexity and limitations of this traditional approach, the concept of "command responsibility," originating from international humanitarian law, has emerged as a potential and more adaptive alternative framework. Unlike futile attempts to hold AI systems themselves accountable or to impose difficult-to-prove direct responsibility on low-level individuals, this approach strategically places the burden of responsibility on the leaders of institutional structures—both military and civilian—who have a legal obligation to exercise effective control over high-risk systems under their authority. At its core, this approach holds that failure to exercise reasonable oversight (due diligence)—even if not directly involved in the specific actus reus—can give rise to criminal liability for commanders or leaders if the system subsequently results in a legal violation. Thus, this concept offers a realistic and normative "middle way," acknowledging the autonomous nature

of technology while reaffirming the non-delegable human responsibility within the oversight and control hierarchy. Its implementation requires clear definitions of who holds effective control over a particular AI system and objective standards for due diligence in the context of developing and deploying complex technologies.

5. DISCUSSION

Theoretically, the findings of this study confirm and deepen the picture of a fundamental tension between the classical criminal law framework—which is intrinsically anthropocentric (human-centric)—and a reality increasingly dominated by non-human and autonomous algorithmic entities. More specifically, the theory of retributive justice, a cornerstone of traditional criminal law, is rooted in retribution for malicious intent (mens rea) of human perpetrators. This principle faces unavoidable philosophical and practical dilemmas when applied to AI systems that operate autonomously through adaptive machine learning and are often not fully predictable by their creators. The resulting tension is not merely operational in nature but also demands a fundamental paradigmatic reconstruction.

The implication is the need to construct a criminal law paradigm no longer exclusively focused on individual subjectivity and culpability in the narrow sense, but one capable of recognizing and articulating the concept of structurally responsible entities. This paradigm shifts the focus from subjective intent to the functions, control mechanisms, and systemic failures within organizational or technological structures that produce harm.

Building such a paradigm requires a thorough re-examination of the theoretical foundations of criminal responsibility. Traditional concepts of act and fault must be expanded to address collective action and systemic responsibility in the creation and deployment of complex AI systems. As presciently emphasized by Manuel G. Velasquez (2003) in the context of corporate moral responsibility, collective entities—such as companies or state institutions—can and should bear moral and legal responsibility when their decision-making structures and operations systematically cause harm, even if no specific individual fault is identifiable[52] (Hu, 2019).

[52] Y Hu, "Robot Criminals," *University of Michigan Journal of Law Reform* 52, no. 2 (n.d.), https://doi.org/10.36646/mjlr.52.2.robot.

This principle has strong and direct relevance to AI. Although AI systems are not "legal persons" in the classical sense, which requires consciousness, they can exhibit concrete and autonomous causal agency in producing outcomes that may meet the elements of certain criminal offences[53];[54]. Accordingly, a framework of accountability must encompass these technological entities through the structures that create, control, and oversee them, while ultimately placing responsibility on the human actors and institutions exercising effective control.

To operationalize this structural and collective approach, the concept of sociotechnical liability is increasingly significant. This model rejects the artificial dichotomy between "humans" and "technology," viewing them instead as inseparable elements of a complex, mutually constitutive system. In such a system, legal responsibility—especially criminal liability—must be understood as dynamically distributed across the network of actors and processes in the AI lifecycle: from design, algorithm development, testing and validation, to implementation, monitoring, updating, and decommissioning.

This approach requires that all actors in the AI value chain—engineers, data scientists, product managers, corporate regulators, and end users with significant authority—be considered within the criminal liability calculus. At the same time, this inclusivity must not compromise fundamental principles of criminal law, particularly the principle of legality (nullum crimen sine lege) and the principle of legal certainty. Therefore, clear definitions of the standard of care, the duty to supervise, and the threshold of negligence triggering criminal liability for each role within the socio-technical system must be rigorously developed and codified in legislation.

By integrating structural responsibility, collective liability based on systemic causal agency, and a sociotechnical framework that proportionally distributes obligations, criminal law can evolve to address the challenges posed by increasingly autonomous digital technologies. This evolution seeks to make criminal law both inclusive and responsive while maintaining the

[53] T C King et al., "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions," *Science and Engineering Ethics* 26, no. 1 (n.d.), https://doi.org/10.1007/s11948-018-00081-0.

[54] M Simmler and N Markwalder, "Guilty Robots? – Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence," *Criminal Law Forum* 30, no. 1 (n.d.), https://doi.org/10.1007/s10609-018-9360-0.

integrity of foundational principles—culpability, proportionality, and deterrence—in a society that is data-driven and algorithmically governed. Ultimately, the transformation is not about punishing machines, but about ensuring that humans and institutions design, implement, and oversee these powerful technologies responsibly.

6. SCIENTIFIC NOVELTY AND RESEARCH CONTRIBUTION

This study presents scientific novelty in contemporary criminal law by raising an issue that has not been studied in depth, namely, criminal liability arising from the impact of artificial intelligence algorithms in the criminal justice system. Until now, most legal studies have focused on the ethical aspects of AI use or the protection of personal data, while conceptual issues regarding the form, basis, and subjects of criminal liability arising from algorithmic decisions remain largely unexplored from a systematic and comparative cross-national criminal law perspective.

Furthermore, this study fills a theoretical gap in criminal law discourse by offering a conceptual approach that combines command responsibility theory and sociotechnical liability as a new basis for formulating structures of criminal responsibility in the context of autonomous digital systems. By integrating principles derived from international humanitarian law and collective responsibility theory in technology ethics, this study successfully builds an argumentative bridge that enables criminal law to undergo a normative transformation without compromising the foundational principles of legality and substantive justice.

On the other hand, the novelty of this research also lies in its methodological approach, namely, a combination of normative and comparative studies of jurisdictions with differing levels of legal technology adoption. By comparing approaches from the United States, the European Union, Germany, and China, this research presents a comprehensive global picture of regulatory fragmentation while offering a conceptual basis for international harmonization. This approach not only adds academic value but also creates opportunities for applying research findings in global policy practice, particularly in the development of international protocols on digital justice.

In practical terms, this research makes a significant contribution to lawmakers, technology regulators, and law enforcement officials. The findings and analysis presented can serve as a basis for developing regulations that are responsive to developments in AI, whether in the form of sectoral regulations, professional codes of conduct for legal practitioners, and operational standards for the use of technology in judicial institutions. Additionally, this research contributes to the discourse on legal education by incorporating a technological dimension into criminal law and criminal procedure law curricula, which have traditionally been dominated by conventional approaches.

Thus, the scientific innovation offered is not only conceptual and normative but also applicable and strategic in responding to the future challenges of criminal law amid digital technology disruption. This study emphasizes that without innovation in legal thinking, the criminal justice system will continue to lag behind in addressing the complexities of the times, and that the law must not only keep pace with technological developments but also frame them within adaptive and responsible principles of justice.

7. CONCLUSION

This study shows that the integration of artificial intelligence (AI) into criminal justice systems presents complex legal challenges, particularly regarding criminal liability for algorithmic decisions that affect individual rights. Through a comparative analysis of jurisdictions such as the United States, the European Union, Germany, and China, this study found that no legal framework explicitly and comprehensively regulates criminal liability for AI system errors in the judicial process. This indicates a legal vacuum that risks fostering uncertainty and injustice, particularly for individuals affected by automated legal decisions.

Furthermore, the findings confirm that the conventional criminal law approach—which relies on individual responsibility through the requirements of mens rea and actus reus—is no longer sufficient in the context of non-human, adaptive, and autonomous algorithmic systems. Therefore, a new construct in criminal liability theory is needed to address this complexity. This study proposes combining the command responsibility and sociotechnical liability approaches as a more relevant conceptual alternative,

as this combination can accommodate the distribution of responsibility within a technological ecosystem involving various actors and automated processes.

From a legal policy perspective, global initiatives are required to develop international standards and protocols governing algorithmic accountability in criminal justice systems. Regulatory harmonization among countries is crucial to prevent regulatory arbitrage and to ensure that the use of AI in the justice sector does not lead to disparities in legal protection across jurisdictions. In this regard, international institutions such as the United Nations and Interpol are expected to play a central role in facilitating dialogue among countries and in promoting the adoption of global principles for digital justice.

REFERENCES

Ahmed Khan, Z, and A Rizvi. "AI Based Recognition Technology and Criminal Justice: Issues and Challenges." *Turkish Journal of Computer and Mathematics Education* 12, no. 14 (n.d.).

Al-Dulaimi, A O M, and M.A.-A.W. Mohammed. "Legal Responsibility for Errors Caused by Artificial Intelligence (AI) in the Public Sector." *International Journal of Law and Management*, n.d. https://doi.org/10.1108/IJLMA-08-2024-0295.

Amelia, S. "Progressive Legal Approach to Modern Community Law Enforcement in Indonesia." *Pancasila and Law Review* 4, no. 1 (n.d.). https://doi.org/10.25041/plr.v4i1.2729.

Aspalter, C. "From Descriptive to Normative Comparative Social Policy: By Way of Conclusion." In *Ideal Types in Comparative Social Policy*, n.d.

Bagaric, M, J Svilar, M Bull, D Hunter, and N Stobbs. "The Solution to the Pervasive Bias and Discrimination in the Criminal Justice: Transparent Artificial Intelligence." *American Criminal Law Review* 59, no. 1 (n.d.).

Blount, K. "Using Artificial Intelligence to Prevent Crime: Implications for Due Process and Criminal Justice." *AI and Society* 39, no. 1 (n.d.). https://doi.org/10.1007/s00146-022-01513-z.

Brennan, T, and W Dieterich. "Correctional Offender Management Profiles for Alternative Sanctions (COMPAS." In *Handbook of Recidivism Risk/Needs Assessment Tools*, n.d. https://doi.org/10.1002/9781119184256.ch3.

Callier, M, and H Callier. "Blame It on the Machine: A Socio-Legal Analysis of Liability in an Blame It on the Machine: A Socio-Legal Analysis of Liability in an AI World AI World." *Technology & Arts Washington Journal of Law* 14 (n.d.).

Carbo, M P B. "Machine Learning Applications in the United States Criminal Justice

System: A Critical Content Analysis of the COMPAS Recidivism Risk Assessment." Nan, n.d.

Custers, B. "AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law." *SSRN Electronic Journal*, n.d. https://doi.org/10.2139/ssrn.4331759.

Dancy, T, and M Zalnieriute. "AI and Transparency in Judicial Decision-Making." *SSRN Electronic Journal*, n.d. https://doi.org/10.2139/ssrn.5331491.

Diamantis, M E. "Vicarious Liability for AI." *Indiana Law Journal* 99, no. 1 (n.d.).

Dupont, B, Y Stevens, H Westermann, and M Joyce. "Artificial Intelligence in the Context of Crime and Criminal Justice." *SSRN Electronic Journal*, n.d. https://doi.org/10.2139/ssrn.3857367.

Eschenbach, W J. "Transparency and the Black Box Problem: Why We Do Not Trust AI." *Philosophy and Technology* 34, no. 4 (n.d.). https://doi.org/10.1007/s13347-021-00477-0.

Fazil, Abdul Wajid, Musawer Hakimi, and Amir Kror Shahidzay. "A Comprehensive Review Of Bias In Ai Algorithms." *Nusantara Hasana Journal* 3, no. 8 (n.d.). https://doi.org/10.59003/nhj.v3i8.1052.

Gaffar, H. "Implications of Digitalization and AI in the Justice System: A Glance at the Socio-Legal Angle." *Law and World* 10, no. 3 (n.d.): 154–177. https://doi.org/10.36475/10.3.14.

Galaz, V, M A Centeno, P W Callahan, A Causevic, T Patterson, I Brass, S Baum, et al. "Artificial Intelligence, Systemic Risks, and Sustainability." *Technology in Society* 67 (n.d.). https://doi.org/10.1016/j.techsoc.2021.101741.

Glavaničová, D, and M Pascucci. "Vicarious Liability: A Solution to a Problem of AI Responsibility?" *Ethics and Information Technology* 24, no. 3 (n.d.). https://doi.org/10.1007/s10676-022-09657-8.

Gravett, W. "Sentenced by an Algorithm — Bias and Lack of Accuracy in Risk-Assessment Software in the United States Criminal Justice System." *South African Journal of Criminal Justice* 34, no. 1 (n.d.). https://doi.org/10.47348/sacj/v34/i1a2.

Gunawan, Y. "Legal Research Perspective through Problem Solution Approach." *International Journal of Science and Society* 5, no. 2 (n.d.). https://doi.org/10.54783/ijsoc.v5i2.705.

Gupta, N. "Artificial Intelligence Ethics and Fairness: A Study to Address Bias and Fairness Issues in AI Systems, and the Ethical Implications of AI Applications." *Revista Review Index Journal of Multidisciplinary* 3, no. 2 (n.d.). https://doi.org/10.31305/rrijm2023.v03.n02.004.

Haim, A. "The Administrative State and Artificial Intelligence: Toward an Internal Law of Administrative Algorithms." *SSRN Electronic Journal*, n.d. https://doi.org/10.2139/ssrn.4498470.

Hamilton, M. "The Biased Algorithm: Evidence of Disparate Impact on Hispanics." *American Criminal Law Review* 56, no. 4 (n.d.).

Hu, Y. "Robot Criminals." *University of Michigan Journal of Law Reform* 52, no. 2 (n.d.). https://doi.org/10.36646/mjlr.52.2.robot.

Karthikeyan, R, C Yi, and M Boudourides. "Criminal Justice in the Age of AI:

Addressing Bias in Predictive Algorithms Used by Courts." In *The Ethics Gap in the Engineering of the Future*, 27–50. Emerald Publishing Limited, n.d. https://doi.org/10.1108/978-1-83797-635-520241003.

King, T C, N Aggarwal, M Taddeo, and L Floridi. "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions." *Science and Engineering Ethics* 26, no. 1 (n.d.). https://doi.org/10.1007/s11948-018-00081-0.

Kirdyashova, E V. *Towards an Interdisciplinary Approach in Public Legal Research*. Courier of Kutafin Moscow State Law University (MSAL, n.d. https://doi.org/10.17803/2311-5998.2023.104.4.041-051.

Kordzadeh, N, and M Ghasemaghaei. "Algorithmic Bias: Review, Synthesis, and Future Research Directions." *European Journal of Information Systems* 31, no. ue 3) (n.d.). https://doi.org/10.1080/0960085X.2021.1927212.

Larsson, S. "The Socio-Legal Relevance of Artificial Intelligence." *Droit et Societe* 103, no. 3 (n.d.). https://doi.org/10.3917/drs1.103.0573.

Laux, J, S Wachter, and B Mittelstadt. "Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act." *SSRN Electronic Journal*, n.d. https://doi.org/10.2139/ssrn.4365079.

Leslie, D. "Tackling COVID-19 through Responsible AI Innovation: Five Steps in the Right Direction." *SSRN Electronic Journal*, n.d. https://doi.org/10.2139/ssrn.3652970.

McKay, C. "Predicting Risk in Criminal Procedure: Actuarial Tools, Algorithms, AI and Judicial Decision-Making." *Current Issues in Criminal Justice* 32, no. 1 (n.d.). https://doi.org/10.1080/10345329.2019.1658694.

Musch, S, M Borrelli, and C Kerrigan. "The EU AI Act: A Comprehensive Regulatory Framework for Ethical AI Development." *SSRN Electronic Journal*, n.d. https://doi.org/10.2139/ssrn.4549248.

Ntoutsi, E, P Fafalios, U Gadiraju, V Iosifidis, W Nejdl, M E Vidal, S Ruggieri, et al. "Bias in Data-Driven Artificial Intelligence Systems—An Introductory Survey." *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 10, no. 3 (n.d.). https://doi.org/10.1002/widm.1356.

Orwat, C, J Bareis, A Folberth, J Jahnel, and C Wadephul. "Normative Challenges of Risk Regulation of Artificial Intelligence and Automated Decision-Making." *SSRN Electronic Journal*, n.d. https://doi.org/10.2139/ssrn.4274828.

Pagallo, U, J Ciani Sciolla, and M Durante. "The Environmental Challenges of AI in EU Law: Lessons Learned from the Artificial Intelligence Act (AIA) with Its Drawbacks." *Transforming Government: People, Process and Policy* 16, no. 3 (n.d.). https://doi.org/10.1108/TG-07-2021-0121.

Putra, P S, and F S Siagian. "The Capability of Artificial Intelligence in Calculating the Losses of Crime Victims." *Kosmik Hukum* 25, no. 2 (n.d.). https://doi.org/10.30595/kosmikhukum.v25i2.25817.

Re, R M, A Solow-Niederman, D Bussel, K Brennan-Marquez, M Kaminski, K Levy, M Minow, et al. "Developing Artificially Intelligent Justice." *Stanford*

Technology Law Review 22 (n.d.).

Rohman, Moh M, N Mu'minin, M Masuwd, and E Elihami. *Methodological Reasoning Finds Law Using Normative Studies (Theory, Approach and Analysis of Legal Materials*. MAQASIDI: Jurnal Syariah Dan Hukum, n.d. https://doi.org/10.47498/maqasidi.v4i2.3379.

Rudin, C, and J Radin. "Why Are We Using Black Box Models in AI When We Don't Need To? A Lesson From An Explainable AI Competition." *Harvard Data Science Review* 1, no. 2 (n.d.). https://doi.org/10.1162/99608f92.5a8a3a3d.

Scherer, M U. "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies." *SSRN Electronic Journal*, n.d. https://doi.org/10.2139/ssrn.2609777.

Shuford, J. "Examining Ethical Aspects of AI: Addressing Bias and Equity in the Discipline." *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023* 3, no. 1 (n.d.): 262–280. https://doi.org/10.60087/jaigs.v3i1.119.

Simmler, M, and N Markwalder. "Guilty Robots? – Rethinking the Nature of Culpability and Legal Personhood in an Age of Artificial Intelligence." *Criminal Law Forum* 30, no. 1 (n.d.). https://doi.org/10.1007/s10609-018-9360-0.

Smuha, N A, E Ahmed-Rengers, A Harkens, W Li, J MacLaren, R Piselli, and K Yeung. "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act." *SSRN Electronic Journal*, n.d. https://doi.org/10.2139/ssrn.3899991.

TSCHIDER, C A. "Beyond the "black Box." *Denver Law Review* 98, no. ue 3) (n.d.). https://doi.org/10.1090/noti1408.

Ulnicane, I. "Artificial Intelligence in the European Union: Policy, Ethics and Regulation." In *The Routledge Handbook of European Integrations*, n.d. https://doi.org/10.4324/9780429262081-19.

Vargas-Murillo, A R, I.N.M.de la A Pari-Bedoya, A M Turriate-Guzman, C A Delgado-Chávez, and F Sanchez-Paucar. "Transforming Justice: Implications of Artificial Intelligence in Legal Systems." *Academic Journal of Interdisciplinary Studies* 13, no. 2 (n.d.). https://doi.org/10.36941/ajis-2024-0059.

Wang, N, and M Y Tian. "Intelligent Justice': AI Implementations in China's Legal Systems," n.d. https://doi.org/10.1007/978-3-030-88615-8_10.

Wischmeyer, T. "Artificial Intelligence and Transparency: Opening the Black Box." In *Regulating Artificial Intelligence*, 75–101. Springer International Publishing, n.d. https://doi.org/10.1007/978-3-030-32361-5_4.

Završnik, A. "Criminal Justice, Artificial Intelligence Systems, and Human Rights." *ERA Forum* 20, no. 4 (n.d.). https://doi.org/10.1007/s12027-020-00602-0.

