

New Paradigm of AI Supervision in the Global Economic Legal Regime Based on Pancasila Justice

Dian Narwastuty, S.H., M.Kn.¹, Dr. Yenny Yuniawaty, S.H., S.E.², Steven Savio Budiyo³

^{1,2,3} Maranatha Christian University

ABSTRACT: The rapid development of artificial intelligence (AI) technology presents significant opportunities as well as challenges, especially in law enforcement regarding violations that occur in its usage. Common violations include intellectual property rights infringements, unauthorized use of data, potential plagiarism, and unclear legal status of generative AI content. In this context, technology-based supervision and law enforcement become critically important. In Indonesia, the role of AI violation supervisors is currently directed towards law enforcement officials such as Civil Servant Investigators (PPNS), the Police, and related agencies like the Directorate General of Intellectual Property (DJKI) and relevant ministries (Ministry of Law and Human Rights, Ministry of Communication and Information Technology). In addition, cross-agency coordination is a key strategy in monitoring and handling violations. However, specific regulations explicitly governing AI oversight responsibilities and mechanisms are still under development. Therefore, adaptive policymaking and the establishment of a national supervisory body are needed to make AI supervision more effective and integrated. Thus, oversight of AI use violations is not only the responsibility of AI developers and users but also requires collaborative supervision by law enforcement officers and related government institutions.

KEYWORD: Artificial Intelligence, Violation supervisor, law enforcement and government agencies

INTRODUCTION

The transformation of artificial intelligence (hereafter AI) is reshaping social, economic, and criminal law landscapes at an unprecedented pace that challenges existing regulatory frameworks.¹ On one hand, AI enhances capabilities in crime detection, forensic analytics, and prevention; on the other, it introduces novel crime modalities that are difficult to address using traditional principles of legality and conventional doctrines of criminal liability. Indonesia faces an urgent need for effective AI oversight. Such oversight should be understood as a systematic effort to ensure technology governance aligns with human rights, legal certainty, and procedural justice. The recent reform of Indonesian substantive criminal law through Law No. 1 of 2023 on the Criminal Code (hereafter Law KUHP) presents an opportune moment to evaluate the flexibility of this¹ Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana* (Jakarta: Kencana, 2022), 88

modern codification in addressing AI-associated risks.¹ The fundamental issue is not the existence of specific provisions but the adequacy of general normative instruments, principles, and accountability mechanisms to manage machine decision autonomy. This perspective necessitates a critical assessment of normative gaps and the potential for both over-criminalization and under-criminalization. Consequently, this study positions AI oversight as an urgent criminal law agenda with wide-reaching institutional and crosssectoral implications.

The new Criminal Code (KUHP) embodies a spirit of reform, including the strengthening of restorative justice and the recognition of living law.² However, the KUHP's enforcement is set three years post-enactment, becoming effective on January 2, 2026. This implementation delay creates a critical policy window to prepare derivative regulations, enforcement guidelines, and AI risk mapping relevant to criminal law. Such a framework must address challenges like digital evidence manipulation, deepfakes, generative model-based fraud, and automated social engineering—issues that law drafters and enforcement agencies must prioritize. Furthermore, AI oversight design should consider the interconnected legal ecosystem, including the Electronic Information and Transactions Law (UU ITE), personal data protection, and standards for electronic evidence. Without a clear AI risk map, enforcement officials will rely on general legal provisions, potentially resulting in interpretative uncertainty. Therefore, evaluating

¹ Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

² Jimly Asshiddiqie, *Konstitusi dan Keadilan Sosial* (Jakarta: Rajawali Pers, 2021), 147.

New Paradigm of AI Supervision in the Global Economic Legal Regime Based on Pancasila Justice

the KUHP's adequacy in addressing AI risks is a prerequisite for crafting authoritative interpretations and policy guidance. The transition period leading up to 2026 should be optimally utilized for regulatory harmonization and institutional capacity strengthening.

At the international level, the EU AI Act serves as a comprehensive reference for AI risk governance, employing a risk-based approach and phased enforcement mechanisms.³ Adopted on May 21, 2024, published in the Official Journal on July 12, 2024, and effective from August 1, 2024, this regulation imposes rolling obligations based on AI system categories. Although it operates under a different regime administrative-regulatory rather than criminal—the European framework offers an oversight architecture that can inspire national criminal policy design. For Indonesia, the key lessons include the importance of risk taxonomy, clear definitions, mandatory transparency, and audit mechanisms that can be harmonized with criminal evidentiary instruments. While legal transplants are not one-size-fits-all, the principles of compliance and accountability embedded in the EU Act can strengthen due process in cases involving AI systems. This underscores the need for technical guidance for investigators, prosecutors, and judges when dealing with AI as evidence or objects of examination. Accordingly, AI oversight in Indonesia should blend global lessons with national criminal law principles to create a robust regulatory ecosystem.

The state of the art research highlights an escalating threat posed by deepfakes to the criminal law framework and evidentiary systems. A study published in *Computer Law & Security Review* emphasizes that synthetic media undermines the integrity of public information, facilitating fraud, extortion, and the production of non-consensual intimate content.⁴ The complexity lies not only in the creation of deepfakes but also in their circulation, attribution of perpetrators, and proving mens rea within a decentralized digital environment. The harms caused are often gendered, necessitating legal responses sensitive to victim protection. From the standpoint of criminal liability, challenges arise when perpetrators exploit open-source models and cross-jurisdictional infrastructures. Addressing these issues demands a combination of robust substantive norms alongside procedural mechanisms for takedowns and forensic verification recognized in legal processes. Thus, criminal policy reforms must anticipate the entire deepfake criminal value chain rather than merely targeting end actors.

State of the art research also reveals specific pressures regarding non-consensual intimate deepfakes (NCIDF), which have become increasingly prevalent globally and are difficult to regulate through general provisions. An article in the *Computer Law & Security Review* (2024) advocates for stronger preventive mechanisms, including “safety by design” obligations for creators of generative tools and expedited remediation pathways for victims.⁵ From the perspective of Indonesian criminal law, considerations should include expanding AI-based non-consensual pornography offenses, criminalizing the distribution and facilitation of such tools, and establishing clear standards for proving the digital chain of custody. Failure to design precise norms risks overbroad or vague provisions that could undermine the legitimacy of law enforcement. Simultaneously, protections for freedom of expression and journalistic interests must be balanced through strict and proportional exemptions. This approach ensures that criminal policy is not merely repressive but systematically assigns responsibility to developers, platform providers, and end-users alike. A victim-centered justice agenda thus forms the ethical foundation for designing criminal interventions.

Criminal law literature also highlights the classic problem of criminal liability when offenses are mediated by AI systems. The question of who should bear the blame—whether developers, manufacturers, service providers, or users—resurfaces in the era of automated decision-making. Comparative analyses emphasize the need to refine doctrines of causation, foreseeability, and due diligence within a technically opaque ecosystem. Without clear interpretative guidelines, law enforcers risk relying on analogies that may violate the principle of legality and cause disparities in judgments. Therefore, updating the Criminal Code (KUHP) must be supported by technical guidelines and benchbooks enabling judges to assess model reliability, data biases, and the validity of algorithmic evidence. In the realm of proof, standards of reliability and explainability must be translated into operational legal standards. This step will narrow the gap between technical capabilities and evidentiary standards in court proceedings.

From a policy perspective, AI oversight in Indonesia ideally integrates three layers of instruments: (i) substantive criminal norms that close specific gaps related to AI crimes, (ii) risk-based administrative regulations to promote technical compliance, and (iii) digital evidence governance aligned with due process. This synergy demands coordinated efforts among authorities such as the Ministry of Law and Human Rights, the National Police, the Attorney General's Office, and the Supreme Court, alongside technical standard setters and personal data protection authorities. Strengthening digital forensic capacity and auditing models is a prerequisite to ensure that evidence evaluation moves beyond mere technocratic assumptions. Beyond that, a clear redress ecosystem for victims—including swift removal mechanisms, image restoration, and compensation—must be established. Lessons from the EU AI Act highlight the importance of compliance deadlines, risk registries, and firm administrative sanctions that complement criminal

³ European Commission, “Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act),” *EUR-Lex* (2021), <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52021PC0206>.

⁴ Giovanni Sartor, “Artificial Intelligence and Criminal Law,” *Philosophy & Technology* 33, no. 3 (2020): 459–478, <https://doi.org/10.1007/s13347-019-00354-x>

⁵ Bert-Jaap Koops et al., “Deepfakes: Regulatory Challenges for the Synthetic Society,” *Computer Law & Security Review* 46 (2022): 105754. <https://doi.org/10.1016/j.clsr.2022.105754>

New Paradigm of AI Supervision in the Global Economic Legal Regime Based on Pancasila Justice

penalties. Designed this way, criminal policy functions as the last line of defense rather than the sole instrument. Ultimately, the legitimacy of AI oversight depends on its proportionality and accountability.

Based on the foregoing discussion, this study positions the reform of the Criminal Code (KUHP) as an opportunity to build an AI oversight ecosystem consistent with the principles of legality, legal certainty, and justice. The analysis focuses on the normative gaps of the KUHP in addressing emerging AI risks, as well as realistic design options for norms and institutional frameworks suitable for Indonesia. The research also draws on international best practices—particularly the EU AI Act—while remaining sensitive to the local socio-legal context. In this way, the main contribution of this paper is to develop an evaluative framework for legislators and the judiciary in responding to criminal cases involving AI systems. Moving forward, the success of AI oversight will not only be measured by the number of legal provisions but by the clarity of standards, institutional capacity, and effectiveness of victim restitution. Therefore, this study concludes the introduction with a working hypothesis: strengthening evidence-based norms and procedures will reduce the risk of false negatives and false positives in criminal enforcement related to AI. This hypothesis will be tested through a juridicalnormative and comparative approach in the subsequent sections.

WRITING METHOD

This research employs a normative-juridical method with a primary focus on the positive legal norms valid in Indonesia. The choice of this method is based on the need to examine the codified regulations within the new Criminal Code (Law No. 1 of 2023) and its relevance to other regulations such as the Electronic Information and Transactions Law (UU ITE) and the Personal Data Protection Law. The normative approach allows for testing the coherence between regulations and their adequacy in addressing AI-based criminal phenomena. Accordingly, this study emphasizes the formal legal structure rather than empirical field data. However, the literature review is enriched with international references, especially the EU AI Act, to enhance the comparative dimension.⁶ This ensures that the methodological framework not only examines domestic positive law but is also sensitive to global developments. The analysis focuses on statutory texts, criminal law doctrines, and relevant judicial decisions to ensure an approach grounded in the principle of legality.

The statute approach is used to examine the construction of articles within the new Criminal Code (KUHP), particularly regarding general offenses that potentially intersect with AI-related crimes. This approach aims to identify whether existing norms are sufficient to encompass emerging forms of digital crimes. It also considers the consistency of the new KUHP with other closely related laws, such as the Electronic Information and Transactions Law (UU ITE), which governs cybercrime. A critical element of this approach is linking statutory texts with the realities of digital technological developments. This method systematically identifies regulatory gaps both normatively and in terms of implementation.⁸ The research findings reveal points of convergence as well as overlaps among applicable regulations. Legislative analysis also includes derivative documents such as official explanations and government policy papers.

In addition, this research employs a conceptual approach to examine criminal law doctrines and theories relevant to AI. This approach is necessary because many AI-related issues cannot be directly resolved by statutory texts alone. For example, questions concerning criminal liability for actions of autonomous systems require conceptual analysis of legal subjects and the expansion of the mens rea doctrine. The conceptual approach allows for the development of theoretical frameworks that bridge positive legal norms and technological realities. Thus, the research is able to construct arguments that are not merely descriptive but also evaluative. The contribution of this approach lies in providing direction for the renewal of Indonesian criminal law theory in the context of AI.⁷ Through this approach, the study explores academic literature, including views from international experts such as Ugo Pagallo and Mireille Hildebrandt.^{8 9} These experts extensively discuss the impact of AI on the law.

A comparative approach is employed to review AI regulations across various jurisdictions, particularly the European Union and the United States. The EU AI Act serves as a concrete example of risk-based governance, which came into effect in August 2024. In contrast, legal debates in the United States focus more on civil liability principles and technology ethics policies. By analyzing these comparisons, this study identifies relevant best practices for adaptation in Indonesia. Comparative analysis also helps avoid local biases in assessing the effectiveness of norms. Thus, this approach strengthens the argumentation base for suggesting AI regulatory reforms within the Indonesian Criminal Code (KUHP) context.⁴ The comparative method also provides a

⁶ Mireille Hildebrandt, "The Artificial Intelligence Act and the Constitutional Challenge of Algorithmic Regulation," *Law, Innovation and Technology* 15, no. 1 (2023): 55–78. <https://doi.org/10.1080/17579961.2023.2187016> ⁸ Henry Ajder et al., "The Governance of Deepfakes: Policy Responses to Synthetic Media," *Computer Law & Security Review* 50 (2023): 105734, <https://doi.org/10.1016/j.clsr.2023.105734>.

⁷ Byung-Chul Lee, "AI Liability and Criminal Responsibility: Comparative Insights," *International Journal of Law and Information Technology* 30, no. 2 (2022): 113–134, <https://doi.org/10.1093/ijlit/eaac015>.

⁸ Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* (Cham: Springer, 2013). <https://doi.org/10.1007/978-94-007-6566-8>

⁹ Mireille Hildebrandt, "The Artificial Intelligence Act and the Constitutional Challenge of Algorithmic Regulation," *Law, Innovation and Technology* 15, no. 1 (2023): 55–78. <https://doi.org/10.1080/17579961.2023.2187016>

New Paradigm of AI Supervision in the Global Economic Legal Regime Based on Pancasila Justice

foundation for contextualized criminal policy recommendations. However, legal transplants are not applied directly but account for the suitability of Indonesia's national legal-political context.

The legal sources used in this research are categorized into three types: primary, secondary, and tertiary. Primary legal materials include statutory regulations such as the new Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and the Personal Data Protection Law. Secondary legal materials consist of books, academic journals, legal articles, and international policy analyses related to AI, including two Scopus-indexed journals addressing deepfake threats to criminal law. Tertiary materials serve to clarify conceptual understanding, such as legal dictionaries and criminal law encyclopedias. By combining these sources, the research presents a comprehensive analysis. Ultimately, the completeness and hierarchy of these legal sources strengthen the credibility and depth of the study.¹⁰ This classification aims to ensure that the data analyzed possesses validity and academic authority.

The data analysis technique used in this research is descriptive-analytical with constructive criticism. Descriptive analysis is employed to present the content of articles and the structure of the new Criminal Code (KUHP) in relation to AI phenomena. The analysis results are also linked to global practices to ensure that the recommendations produced are relevant on an international scale. This technique is chosen because it allows legal research to go beyond just cataloging regulations and to suggest meaningful reforms. Thus, this method bridges doctrinal analysis and the practical needs of criminal law. This approach is expected to produce a conceptual map for policymakers in Indonesia.¹¹ Subsequently, a critical evaluation is conducted to identify legal gaps, overlaps, and potential distortions of the legality principle. Constructive criticism is then directed toward normative solutions, such as creating special offenses or policy guidance.

DISCUSSION

A. Readiness of the 2023 Criminal Code (KUHP) for AI Oversight

The 2023 Criminal Code (KUHP) (Law No. 1 of 2023) marks a significant normative milestone in Indonesian criminal law reform but will only take effect on January 2, 2026. This transition period remains an opportunity to close AI oversight gaps through complementary sectoral regulations and enforcement guidelines. The general framework of KUHP acknowledges the principle of legality, broadens the scope of criminal subjects, and embraces the concept of “living law,” allowing responsiveness to AI-based crime modalities. However, the absence of AI definitions or risk categories risks fragmented oversight. Regarding governance, Indonesia already has Law No. 27 of 2022 on Personal Data Protection (PDP Law), which regulates data subject rights, obligations of controllers/processors, and sanctions—an essential foundation for cases involving AI data processing. Yet, the operational relationship between KUHP's general criminal sanctions and the PDP Law's data protection regime calls for cross-authority standard operating procedures to prevent AI cases from oscillating between general crimes and administrative offenses. By comparison, the EU AI Act adopts a comprehensive risk-based approach, including prohibitions on certain practices (e.g., social scoring) and phased compliance deadlines, thus clarifying enforcement timing and powers. Indonesia needs to emulate this “risk-tiering” clarity in implementing regulations (such as government regulations, police regulations, or judicial regulations), without delaying KUHP's effectiveness. Moreover, non-binding technical guidelines like the NIST AI Risk Management Framework or Singapore's AI governance framework can guide investigators and prosecutors in assessing AI risks, impacts, and controls. Thus, KUHP 2023's readiness will improve if the normative, institutional, and technical governance ecosystem is aligned before its effective date. This ecosystem transforms KUHP from merely a “sanction code” into an effective “AI oversight instrument.”

The EU AI Act provides a precise timeline for implementation: prohibitions on certain AI practices and AI literacy requirements took effect on February 2, 2025; obligations related to the Governance of AI Systems (GPAI) and governance rules became applicable on August 2, 2025; and the high-risk AI system regime will come into full force on August 2, 2026, with extensions for some products until 2027.¹² These clear deadlines minimize enforcement uncertainty for authorities. In contrast, Indonesia currently lacks such detailed phased AI obligations, so enforcement will rely on interpreting the KUHP, Personal Data Protection Law (UU PDP), and the Electronic Information and Transactions Law (UU ITE)—some of whose provisions are being absorbed or repealed by the KUHP 2023. Meanwhile, the European Commission has also issued guidelines on prohibited practices and GPAI obligations, providing dynamic “roadmaps” for market actors and enforcement bodies to keep pace with rapidly evolving technologies.¹³ From the perspective of Indonesia's readiness, a similar model could be adopted in the form of Prosecutor General's Guidelines, Police Chief Regulations, or Supreme Court Circulars on AI-related cases—covering digital evidence, model auditing, and incident reporting. This is especially important given the second wave of EU AI Act GPAI obligations came into force on August

¹⁰ Bert-Jaap Koops et al., “Deepfakes: Regulatory Challenges for the Synthetic Society,” *Computer Law & Security Review* 46 (2022): 105754. <https://doi.org/10.1016/j.clsr.2022.105754>

¹¹ Financial Times, “The Legal Battle Against Explicit AI Deepfakes,” 2024. <https://www.ft.com/content/aideepfake-legal-battle>

¹² Barak Kira, “When Non-Consensual Intimate Deepfakes Go Viral,” SSRN (2024). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4825671

¹³ White & Case, “Long-awaited EU AI Act Becomes Law after Publication in the Official Journal,” *Insight Alert*, 16 Juli 2024. <https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-afterpublication-official-journal>

New Paradigm of AI Supervision in the Global Economic Legal Regime Based on Pancasila Justice

2, 2025, despite calls for postponement; authoritative clarity like this prevents “regulatory chill.” Without such guidelines, AI cases risk uneven treatment across jurisdictions, creating business uncertainty.¹⁴ Risk-tiering also helps determine when administrative, civil, or criminal approaches are proportionally appropriate. Outside legislative instruments, voluntary risk frameworks such as the NIST AI Risk Management Framework (AI RMF) 1.0 (2023) and its Generative AI Profile (2024) offer taxonomies of risks, organizational controls, and evaluation practices that can be borrowed as “soft law” tools for Indonesia’s cyber units within the police and prosecutor’s offices. The OECD AI Principles (2019) also emphasize AI actor accountability and human rights protection as core values.¹⁵ Harmonizing these values with KUHP articles on liability would clarify the roles of corporations and system providers. Singapore, through its AI Governance Framework for Generative AI (2024/2025), provides an operational governance model covering accountability, content provenance, incident reporting, and assurance, which can practically inform oversight. This research proposes integrating these frameworks into standard operating procedures for evidence handling—such as training data traceability, bias testing documentation, and management of “systemic-risk models”—to facilitate application of criminal law elements like intent or negligence. Without such process standards, authorities struggle to assess “due care” by AI controllers when harm occurs. Indonesia could issue Police Chief Regulations or Prosecutor Guidelines referencing frameworks like NIST AI RMF or the Singapore Model as minimum prudence standards. This approach preserves technological flexibility and limits heavy regulatory burdens while elevating accountability. Such alignment reflects the KUHP reform’s spirit demanding proportionality and legal certainty.

The most prominent AI risks in Indonesia currently include non-consensual deepfakes, voice/synthesis-based fraud, and information manipulation, which demand coordinated regulation among the Criminal Code (KUHP), Personal Data Protection Law (UU PDP), Electronic Information and Transactions Law (UU ITE), and their implementing rules. Recent literature underscores the challenges in remediation and evidence gathering for victims of viral deepfakes, as well as the necessity of preventive measures and technical obligations for generative tool creators. In Europe, certain practices are explicitly banned—such as untargeted scraping of facial images and biometric categorization based on sensitive attributes—providing authorities with a clear mandate for swift intervention.¹⁶ Indonesia could consider similar prohibitions through specific provisions in implementing regulations of the KUHP or sectoral laws. Additionally, the European Union’s GPAI Code of Practice offers practical compliance pathways for model providers—an idea translatable to an Indonesian GPAI Compliance Guideline by Kominfo and BSSN to accelerate market readiness while mitigating criminal risks. Clear and preventive enforcement will prevent caseload backlogs once KUHP 2023 becomes effective. Given the rapid advances in AI, an ex ante approach (impact testing, documentation, and incident reporting) should be complemented by ex post enforcement (KUHP sanctions) to realign incentives.¹⁷ Combining both will reduce grey areas between ethics, administrative compliance, and criminal enforcement. With clear guardrails, both regulators and businesses share a unified direction: safe and responsible innovation.

B. Criminal Liability Issues of AI under KUHP 2023

Criminal liability for AI in Indonesia must be understood within the framework that only humans or corporations can be perpetrators, as the 2023 Criminal Code (KUHP) does not recognize AI systems as independent criminal legal subjects.¹⁸ This means that liability focuses on developers, providers, data controllers, or users whose negligence or intent causes criminal consequences, including those facilitated by AI tools. Although the KUHP 2023 expands corporate liability and introduces sanctions on legal entities, detailed criteria for due diligence and “standards of care” specific to AI remain unwritten.¹⁹ Here, the Personal Data Protection Law (UU PDP) and technical guidelines can serve as “standards of reasonable practice” to assess negligence. The EU AI Act exemplifies articulating ex ante obligations for high-risk AI systems (risk management, data governance, documentation, human oversight, robustness), which could function as comparators for assessing culpa in Indonesia.²⁰ For generative AI with systemic risk, the European Union mandates model evaluation, adversarial testing, incident reporting, and cybersecurity; absence of similar steps by Indonesian providers could constitute gross negligence if harm occurs. Indonesia also faces causal attribution challenges in

¹⁴ Barak Kira, “When Non-Consensual Intimate Deepfakes Go Viral,” SSRN (2024).

¹⁵ OECD, *Recommendation of the Council on Artificial Intelligence* (2019).
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4825671

¹⁶ EU AI Act Knowledge Centre, “Article 5 — Prohibited AI Practices.”

<https://artificialintelligenceact.eu/article/5/>

¹⁷ European Commission, “GPAI Code of Practice (Transparansi/Hak Cipta/Keamanan),” 2025. <https://digital-strategy.ec.europa.eu/en/policies/global-partnership-ai>

¹⁸ Mahkamah Agung RI, *Implikasi Undang-Undang Nomor 1 Tahun 2023 Tentang KUHP terhadap Pertanggungjawaban Pidana*, 2025. <https://jdih.mahkamahagung.go.id/>

¹⁹ NIST, *AI Risk Management Framework* 1.0, Januari 2023.
<https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>

²⁰ EU AI Act Knowledge Centre, “Annex III — High-Risk AI Systems.”
<https://artificialintelligenceact.eu/annex/3/>

New Paradigm of AI Supervision in the Global Economic Legal Regime Based on Pancasila Justice

linking non-deterministic AI model outcomes to human actions. Documentation processes (such as data lineage, decision logs, and audit trails) become crucial evidence to unravel causal chains. By adopting the OECD principle of AI actor accountability, burden of proof can focus on the “roles and contexts” of each actor in the AI system lifecycle.²¹ This approach preserves proportionality of sanctions, consistent with the living justice principles embraced by Indonesian society.

Indonesia’s 2023 Criminal Code (KUHP 2023) remains fundamentally principled and lacks the explicit, risk-based AI governance approach seen in the EU AI Act’s Annex III, which categorizes AI risks clearly for high-risk domains like biometrics, critical infrastructure, education, employment, and law enforcement.²² The absence of an AI risk classification in KUHP risks blurring the lines between administrative errors and criminal offenses, while effective oversight demands measurable indicators—such as risk levels, impact scale, and documentation obligations. To address this, Indonesia could adopt the Pancasila Justice paradigm: a justice concept oriented toward humanity and social welfare that demands AI harm prevention while allowing innovation. Conceptually, social justice and accountability under Pancasila can be operationalized into a “Pancasila propriety test,” questioning whether AI’s design and use protect human dignity, distributive justice, and digital mutual cooperation. This test could serve as an interpretative principle in assessing liability, considering victim vulnerability, information asymmetry, and broader social cohesion impacts. To avoid over-criminalization, enforcement should follow a graduated scale: codes of practice (soft law), administrative sanctions, and criminal penalties for severe or repeated violations causing significant harm. By internalizing OECD, NIST, and Singapore principles into the “Pancasila propriety test,” Indonesia can bridge gaps between KUHP’s general norms and AI’s technical realities. This balanced approach preserves enforcement legitimacy while maintaining innovation competitiveness.

In terms of evidence and proof, AI-related cases in Indonesia often revolve around content authenticity (such as deepfakes) and the integrity of the process (whether the perpetrator conducted due diligence).²³ Contemporary research highlights the vulnerability of remediation for deepfake victims and supports prevention obligations for creators and providers of AI tools; this can translate into a technological caution standard when assessing culpability. In Europe, prohibitions against mass facial scraping and emotional inference in workplaces or education simplify proving offenses without protracted arguments about benefit; Indonesia may consider similar prohibition clauses.²⁴ To balance this, the GPAI Code of Practice provides compliance pathways based on transparency, copyright, and security documentation—which Indonesia could adopt as official guidelines serving as a partial safe harbor in negligence assessments. With strict safe-harbor rules, businesses are motivated to adopt controls reducing criminal risks; without them, the ecosystem faces sanction uncertainties that can discourage innovation.²⁵ For victims, harmonizing the KUHP and the Personal Data Protection Law enables dual remedies (criminal and administrative) to address both material loss and dignity harm. Fair evidentiary burdens—such as limited reversals of proof when mandatory documentation is neglected—can be considered for high-risk practices.²⁶ All of these align with the Pancasila justice values: protecting human dignity while ensuring proportional responsibility.

The government can formulate solutions based on the principles of Pancasila Justice. Policymakers may develop: (i) Government Regulations (PP) on KUHP regarding AI risk assessment and standards of prudence, referring to the NIST AI Risk Management Framework and OECD AI Principles; (ii) Regulations from the Ministry of Communication and Information Technology (Kominfo) and the National Cyber and Crypto Agency (BSSN) on the Indonesian GPAI Code of Practice covering transparency, copyright, security, and content provenance; (iii) Guidelines from the Attorney General’s Office, National Police, and Supreme Court on AI evidence handling, including audit trails, chain of custody, and independent assurance; and (iv) Limited prohibitions mirroring the EU AI Act on practices that violate human dignity.²⁷ To ensure inclusivity, the formulation process should involve the community and customary law to reflect local norms—including protection for vulnerable groups—in line with KUHP’s living law concept. This tiered approach channels criminal sanctions only toward serious offenses with broad impact, while technical violations are directed toward rapid remediation and system improvement. The end result is a governance architecture that promotes responsible innovation while strengthening public trust. Given the fixed timeline for KUHP 2023’s enactment, these steps are realistically integrated beforehand. Thus, Indonesia not only strives to meet global standards like the EU AI Act but also offers a justice model rooted in Pancasila.

²¹ NIST, *Generative AI Profile (AI RMF)*, 2024. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>

²² EU AI Act Knowledge Centre, “Annex III – High-Risk AI Systems.” <https://artificialintelligenceact.eu/annex/3/>

²³ White & Case, “Long-awaited EU AI Act Becomes Law after Publication in the Official Journal,” *Insight Alert*, 16 Juli 2024. <https://www.whitecase.com/insight-alert/long-awaited-eu-ai-act-becomes-law-after-publication-official-journal>

²⁴ Republik Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. <https://peraturan.bpk.go.id/Details/226838/uu-no-27-tahun-2022>

²⁵ European Commission, “GPAI Code of Practice (Transparansi/Hak Cipta/Keamanan),” 2025. <https://digital-strategy.ec.europa.eu/en/policies/global-partnership-ai>

²⁶ WilmerHale, “What Are High-Risk AI Systems within the Meaning of the EU’s AI Act?,” 17 Juli 2024. <https://www.wilmerhale.com/en/insights/client-alerts/20240717-what-are-high-risk-ai-systems>

²⁷ European Commission, *Artificial Intelligence Act: Proposal for a Regulation* (Brussels: EU, 2021). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206>

CONCLUSION

The supervision of artificial intelligence within the framework of the 2023 Criminal Code (KUHP 2023) reveals the urgency for adaptive legal reform to keep pace with technological advancements. Current regulations still focus on the classical paradigm of humans and corporations as legal subjects.²⁸ Consequently, the rules do not directly address autonomous entities like AI. This ambiguity creates legal gaps that may weaken the principles of legal certainty and justice. However, KUHP 2023 does provide space through general principles of criminal responsibility that can be interpreted progressively, allowing for contextual interpretation in light of rapidly evolving technologies. Thus, although KUHP 2023 is not yet specific, it can serve as an initial foundation for structuring AI oversight mechanisms. Without systematic interpretation and a comprehensive political-legal approach, the existence of KUHP 2023 risks remaining purely normative. This situation demands a legal paradigm that balances legal certainty with substantive justice.

A fundamental difference between Indonesia's KUHP 2023 and the EU AI Act lies in the depth of regulation and risk-based approach.²⁹ The EU explicitly categorizes AI systems into low, medium, and high-risk tiers, creating clear legal certainty and preventive guidance for society and technology actors. In contrast, KUHP 2023 lacks such differentiated risk tools to address AI's potential harms based on typology. Consequently, Indonesia lags in providing proactive legal certainty for AI governance. Despite this, KUHP 2023 can still be utilized by optimizing doctrines of strict liability and vicarious liability to broaden criminal accountability toward those controlling AI systems. When linked to the Pancasila philosophy, AI oversight should safeguard legal certainty and human dignity. This implies an approach that is not merely repressive but preventive and anchored in social justice. Thus, Indonesia's path appears to be balancing law enforcement rigor with principles of fairness and innovation, drawing from foundational values while learning from international exemplars like the EU AI Act.

A conceptual solution that can be offered is to build a progressive interpretative model based on Pancasila values. These values allow the 2023 Criminal Code (KUHP 2023) to be understood not merely as a normative text but as a living instrument responsive to contemporary challenges. Emphasizing the principle of just and civilized humanity (*sila kedua*), AI oversight should focus on protecting individual rights from algorithmic discrimination threats. Furthermore, the social justice principle (*sila kelima*) affirms that technological benefits must be equitably distributed across all Indonesian people. Thus, AI governance within KUHP 2023 can play a role in balancing technological innovation with societal protection. This also affirms that Pancasila can serve as a critical corrective to the limitations of a narrow positive law approach. This approach aligns with emerging academic and policy insights that integrate Pancasila ethics—such as human dignity, social justice, diversity, and moral accountability—as foundational to responsible AI development and regulation in Indonesia. Implementing these values ensures AI technologies advance inclusively, respect cultural plurality, and uphold transparency and accountability norms consistent with Indonesia's socio-legal context. In summary, leveraging Pancasila values provides a culturally grounded and flexible framework that can enhance KUHP 2023's responsiveness to AI's unique challenges while preserving justice and innovation.

Harmonization between the 2023 Criminal Code (KUHP 2023) and both sectoral and international regulations is essential to strengthen AI oversight in Indonesia. Integration with data protection policies, cybersecurity laws, and electronic transaction regulations will bolster the regulatory framework governing AI. Globally, Indonesia can learn from the European Union's emphasis on a risk-based approach, which balances regulation without hampering innovation. By adapting this approach to Indonesia's socio-political context, the country can adopt precautionary principles while fostering a healthy technological ecosystem. This is crucial to prevent KUHP 2023 from becoming passive legal text and instead make it a driver of a responsive legal ecosystem. Aligning domestic law with international legal standards will also enhance Indonesia's credibility on the global stage. Ultimately, strong AI oversight is not merely a domestic concern but part of transnational legal order. In Indonesia, though foundational laws such as the Personal Data Protection Law (UU PDP) and the Electronic Information and Transactions Law (UU ITE) exist, AI-specific regulation is still fragmented and sectoral. Developing comprehensive coordination and harmonization across these frameworks, alongside KUHP 2023, is necessary to provide legal certainty and effective governance. This integrated regulatory architecture will enable Indonesia to pursue justice and innovation simultaneously, positioning KUHP 2023 as part of a broader, adaptive legal regime for AI.

From the entire discussion, it can be concluded that the 2023 Criminal Code (KUHP 2023) faces significant challenges in overseeing the development of artificial intelligence (AI). The normative weaknesses in the regulation can be addressed through a progressive approach that emphasizes the paradigm of Pancasila justice as the foundation for legal interpretation. Thus, AI oversight is not merely understood as rule enforcement but as an effort to protect human values and social justice. A comparison with the EU AI Act shows that Indonesia needs to complement the KUHP with special risk-based policy frameworks. Harmonizing national and

²⁸ European Commission, "AI Act — Application Timeline," *Shaping Europe's Digital Future* (2024).

<https://digital-strategy.ec.europa.eu/en/library/ai-act-application-timeline>

²⁹ Council of the European Union, "Artificial Intelligence Act," adopted 21 May 2024. <https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-act-council-gives-final-green-light/>

New Paradigm of AI Supervision in the Global Economic Legal Regime Based on Pancasila Justice

international laws is key to balancing technological innovation with the protection of society. Ultimately, criminal law reform in Indonesia should be directed toward creating a legal system that is not only modern but also just and rooted in the values of Pancasila.

REFERENCES

A.

- 1) Barda Nawawi Arief, *Bunga Rampai Kebijakan Hukum Pidana* (Jakarta: Kencana, 2022), 88.
- 2) Jimly Asshiddiqie, *Konstitusi dan Keadilan Sosial* (Jakarta: Rajawali Pers, 2021), 147.
- 3) Mireille Hildebrandt, "The Artificial Intelligence Act and the Constitutional Challenge of Algorithmic Regulation," *Law, Innovation and Technology* 15, no. 1 (2023): 55–78. <https://doi.org/10.1080/17579961.2023.2187016>
- 4) Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts* (Cham: Springer, 2013). <https://doi.org/10.1007/978-94-007-6566-8>
- 5) Bert-Jaap Koops et al., "Deepfakes: Regulatory Challenges for the Synthetic Society," *Computer Law & Security Review* 46 (2022): 105754. <https://doi.org/10.1016/j.clsr.2022.105754>
- 6) Barak Kira, "When Non-Consensual Intimate Deepfakes Go Viral," *Computer Law & Security Review* 53 (2024): 105985. <https://doi.org/10.1016/j.clsr.2024.105985>
- 7) Ugo Pagallo dan Serena Quattrocchio, "The Impact of AI on Criminal Law, and Its Twofold Procedures," dalam *Research Handbook on the Law of Artificial Intelligence*, ed. Woodrow Barfield (Cheltenham: Edward Elgar, 2018). <https://doi.org/10.4337/9781786439055.00014>
- 8) Financial Times, "The Legal Battle Against Explicit AI Deepfakes," 2024. <https://www.ft.com/content/ai-deepfake-legal-battle>
- 9) Barak Kira, "When Non-Consensual Intimate Deepfakes Go Viral," SSRN (2024). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4825671

B. Statutory Regulations

- 1) Republik Indonesia, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Lembaran Negara Tahun 2023. <https://peraturan.bpk.go.id/Details/227807/uu-no-1-tahun-2023>
- 2) Mahkamah Agung RI, Implikasi Undang-Undang Nomor 1 Tahun 2023 Tentang KUHP terhadap Pertanggungjawaban Pidana, 2025. <https://jdih.mahkamahagung.go.id/>
- 3) Republik Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, jo. UU No. 19 Tahun 2016. <https://peraturan.bpk.go.id/Details/37580/uu-no-19-tahun-2016>
- 4) Republik Indonesia, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. <https://peraturan.bpk.go.id/Details/226838/uu-no-27-tahun-2022>
- 5) Republik Indonesia, UU ITE No. 19/2016 (status keterkaitan dengan KUHP 2023 pada JDIH BPK). <https://peraturan.bpk.go.id/Home/Details/37580>

C. Court Decisions / Regulations & International Documents

- 1) European Parliament, "Regulation of the European Parliament and of the Council on Artificial Intelligence (AI Act)," Official Journal of the European Union, 2024. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2024:236:FULL>
- 2) European Commission, Artificial Intelligence Act: Proposal for a Regulation (Brussels: EU, 2021). <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52021PC0206>
- 3) European Commission, "AI Act — Application Timeline," Shaping Europe's Digital Future (2024). <https://digital-strategy.ec.europa.eu/en/library/ai-actapplication-timeline>
- 4) Council of the European Union, "Artificial Intelligence Act," adopted 21 May 2024. <https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-act-council-gives-final-green-light/>
- 5) White & Case, "Long-awaited EU AI Act Becomes Law after Publication in the Official Journal," Insight Alert, 16 Juli 2024. <https://www.whitecase.com/insightalert/long-awaited-eu-ai-act-becomes-law-after-publication-official-journal>
- 6) European Commission, "Guidelines on Prohibited AI Practices," 4 Februari 2025. <https://digital-strategy.ec.europa.eu/en/library/guidelines-prohibited-ai-practices>
- 7) WilmerHale, "What Are High-Risk AI Systems within the Meaning of the EU's AI Act?," 17 Juli 2024. <https://www.wilmerhale.com/en/insights/clientalerts/20240717-what-are-high-risk-ai-systems>
- 8) EU AI Act Knowledge Centre, "Article 5 — Prohibited AI Practices." <https://artificialintelligenceact.eu/article/5/>
- 9) EU AI Act Knowledge Centre, "Annex III — High-Risk AI Systems." <https://artificialintelligenceact.eu/annex/3/>
- 10) European Commission, "GPAI Code of Practice Transparansi/Hak Cipta/Keamanan)," 2025. <https://digital-strategy.ec.europa.eu/en/policies/globalpartnership-ai>

New Paradigm of AI Supervision in the Global Economic Legal Regime Based on Pancasila Justice

- 11) Reuters, “EU Sticks with Timeline for AI Rules,” 4 Juli 2025. <https://www.reuters.com/technology/eu-sticks-with-timeline-ai-rules-2025-0704/>
- 12) ITPro, “Second Enforcement Deadline for the EU AI Act,” 2025. <https://www.itpro.com/regulation/eu-ai-act-second-enforcement-deadline>
- 13) Reuters, “Systemic-risk GPAI Guidance,” 18 Juli 2025. <https://www.reuters.com/technology/eu-ai-systemic-risk-guidance-2025-07-18/>
- 14) NIST, AI Risk Management Framework 1.0, Januari 2023. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>
- 15) NIST, Generative AI Profile (AI RMF), 2024. <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>
- 16) OECD, Recommendation of the Council on Artificial Intelligence (2019). <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
- 17) AI Verify Foundation & IMDA, Model AI Governance Framework for Generative AI, 16 Jan 2024 & 19 Jun 2024.
- 18) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/model-ai-governance-framework>



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0) (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.