DRAFTING LAWS FOR THE LIFELESS: A LEGAL FRAMEWORK FOR CRIMINAL LIABILITY AND PUNISHMENT FOR ARTIFICIAL INTELLIGENCE

Wawan Fransisco
Universitas Bina Insan
wawanfransisco@gmail.com

Abstract

In this modern era, Artificial Intelligence (AI) has penetrated almost every aspect of life, offering tremendous benefits to humanity. However, like two sides of a coin, AI also presents serious risks, including its use in criminal act. For example, AI-powered lethal autonomous weapons can select targets and make killing decisions without human involvement. Similarly, autonomous cars can cause fatal accidents. A crucial question arises in these cases: Who should be held accountable? Is it the developer, the owner, the user, the supervisor, or even the AI itself? In criminal law, liability requires two main elements: *actus reus* (wrongful act) and *mens rea* (malicious intent). However, is it possible for AI to have malicious intent? Can AIs be treated as legal subjects worthy of punishment? This article critically examines the legal dilemma and offers three conceptual models to enable AI criminal liability. In addition, it analyses the possibility of imposing sanctions, such as imprisonment and fines, on non-human entities, as well as the relevance of theories of punishment in the context of AI. An analysis of the benefits and risks of punishing AI is also comprehensively outlined as an alternative to other solutions.
Keywords: Artificial Intelligence, Legal Personality, Criminal Liability, Mens Rea, Punishment.

Introduction

Artificial intelligence (AI) is increasingly being used in criminal act. AI is becoming increasingly involved in cybercrimes and illegal drug

dealing on the dark web.[1] Autonomous self-driving vehicles have been implemented in numerous nations[2]. Elaine Herzberg, a homeless woman, lost her life in an Uber test vehicle accident in Arizona, USA, in March 2018.[3] This was the first time a self-driving automobile had killed someone in a traffic accident. Many nations' armed forces are using autonomous weapons.[4] These lethal weapons are capable of identifying their targets, analyzing different tactics in a split second, and killing individuals without human assistance.[5] No nation's criminal justice system can effectively punish those responsible for these AI-powered autonomous weapons. AI is now rapidly becoming more and more integrated into our daily lives. An AI robot employed at a Kawasaki motorcycle manufacturing facility in Japan killed a worker there in 1981.[6] Nearly 40 years have passed since then. Rapid technical advancements have elevated AI's cognitive capacity to a new level. AI has the potential to endanger Society if it is not adequately regulated. Who should be held accountable for crimes perpetrated by artificial intelligence? AI has already participated in several actions that would be illegal if carried out by a human. Furthermore, it is highly challenging to track down the crimes that AI has committed. The primary reason of society fears AI is that it is not yet covered by criminal law.

The development of autonomous artificial intelligence poses fundamental challenges to criminal law systems, which are built on an anthropocentric paradigm. First, there is a legal personhood gap,

---

[1] Raghu Raman et al., Dark web research: Past, present, and future trends and mapping to sustainable development goals, *Heliyon*, 9, (2023). page 9. DOI:10.1016/j.heliyon.2023.e22269

[2] Alireza Shahidi et al., Barriers to the sustainable adoption of autonomous vehicles in developing countries: A multi-criteria decision-making approach, *Heliyon*, 9, (2023), page 2. DOI:10.1016/j.heliyon.2023.e15975

[3] Helen Stamp, The Reckless Tolerance Of Unsafe Autonomous Vehicle Testing: Uber's Culpability For The Criminal Offence Of Negligent Homicide, *Journal of Law, Technology, & the Internet*, volume 15, issue 1, (2024) page 75. https://scholarlycommons.law.case.edu/jolti/vol15/iss1/2/

[4] Eric Rosenbach, Ethan Lee, Bethany Russell (2025). *The Autonomous Arsenal in Defence of Taiwan,* (Harvard Kennedy School, Cambridge, 2025) page 3.

[5] Daniele Amoroso et al., Autonomy in Weapon Systems: The Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy, *Democracy*, Volume 49, (2023), page 33.

[6] Philip Frana, Michael Klein, *Encyclopedia of Artificial Intelligence: The Past, Present, and Future of AI*, (Santa Barbara, California: ABC-CLIO, LLC, 2021), page 2.

whereby Indonesian criminal law currently only recognizes humans and corporations as legal subjects that can be held accountable for their actions. The absence of a normative construction regarding the legal status of autonomous AI raises problems in the Application of the principle of legality, giving rise to an urgent need to recognize a new sui generis category of legal subjects to fill the void in the attribution of responsibility for losses caused by AI. Second, there is the challenge of applying the principle of fault (mens rea) as an essential element of criminal liability. Autonomous AI operates without consciousness or free will, so the traditional interpretation of intent and negligence cannot be directly applied. A doctrinal update is necessary to develop the concept of algorithmic mens rea or a form of culpa that is relevant to the characteristics of autonomous systems, ensuring the principle of fault remains normatively intact while maintaining legal certainty. Third, a punishment crisis has arisen because conventional criminal sanctions in the form of imprisonment and fines cannot be applied to non-human entities. To ensure the objectives of punishment, both in terms of general prevention, specific prevention, and retribution, the legal system must formulate alternative forms of sanctions that are appropriate to the nature of AI, such as deactivation, functional restrictions, data erasure, or source code modification, while still guaranteeing the principles of justice and proportionality.

Thus, the complexity of AI criminal liability necessitates reform comprehensively and normatively, ensuring that criminal law remains adaptable to the development of autonomous technology without compromising the fundamental principles of criminal law.

Research Method

Because of analyzing laws, literature, journals, and papers related to the topic under review, this paper uses the normative legal writing method.[7] The information used in this study is secondary data, namely, information obtained from literature studies and documentation, which is available in the form of literature or documentation and the result of research and processsed by other parties.

According to Peter Mahmud, legal research is a process of discovering legal rules, principles, and doctrines to answer legal issues

[7] Soerjono Soekanto. *Pengantar Penelitian Hukum*. UI Press. Jakarta. 1989, page 7.

that arise.[8] Research methodology is an absolute element that must be present in any research. It serves as a guideline for scientists in studying, analysing, and understanding a phenomenon or issue being researched to achieve the desired and attainable objectives.[9]

The use of normative methods allows for a comprehensive examination of AI criminal liability in Indonesian positive law. This method provides a framework for examining legal issues, analysing existing regulations, and developing policy recommendations to address new challenges arising from technological advances. By integrating the latest developments in AI regulation worldwide, this study provides a comprehensive overview of the way of legal framework for AI criminal liability in Indonesia can be developed. The study encompasses an analysis of international policies, case studies from various countries, and an examination of existing challenges and opportunities within the local context.

Discussion

1. AI-related crimes

The primary issue with AI-related crimes is not only identifying the perpetrator but also determining which legal entity should be held responsible. Establishing the responsible legal subject is a matter of policy that must be clearly defined and understood. Questions arise as to whether fault (mens rea) can still attach to human developers, owners, or users based on negligence, knowledge of risks, or intentional actions. Thus, AI criminal liability requires a normative framework identifying relevant actors and liability standards. Historically, machines have caused harm due to operator error or defects, and criminal responsibility falls on the human user or supervisor, not the tool itself. For example, a knife used in a crime implicates the user, not the knife. AI differs from conventional tools because it can act autonomously, processing inputs, setting goals, evaluating outcomes, and adjusting behavior without human intervention. When AI commits a crime independently, no human can be held accountable, creating a serious risk that such crimes will go unpunished in a civilized society.

Since AI is still frequently not completely independent, crimes

[8] Peter Mahmud Marzuki. Penelitian Hukum. Kencana Prenada. Media Group. Jakarta. 2011, page 35.

[9] Soerjono Soekanto. *Pengantar Penelitian Hukum*. page 7.

involving AI can be attributed to personal accountability.[10] For example, if AI software designed to steal private data causes network damage, its creator remains accountable. However, if the AI begins acting autonomously, stealing data, damaging systems, or launching independent attacks, the situation becomes more complex.

Due to AI's increasing autonomy and complexity, enabling it to participate in crimes without human intervention, it is currently challenging to identify the person responsible for many illegal behaviours.[11] Since AI development involves thousands of contributors, holding a single individual accountable for AI crimes is difficult. AI may become autonomous and misuse knowledge gained from billions of sources, even if created for beneficial purposes. Developers cannot be blamed when such misuse is unforeseeable, as criminal responsibility requires both mens rea and actus reus, or at least negligence.

As AI becomes more sophisticated, autonomous, and capable of making independent decisions, amendments to the criminal code are needed; otherwise, autonomous entities could escape liability. Through the rise of AI-related crimes, particularly in autonomous weapons, the dark web, and self-driving cars, urgent regulations are required to limit AI misuse.

2. AI Criminal Liability Models

The criminal culpability of the individual (natural or artificial, such as a company or artificial intelligence) is the most crucial question in criminal law. someone will be held criminally liable, two requirements must be met. 'Actus reus' refers to the illegal act (or omission), and 'mens rea' refers to the criminal intent or mental component.[12] A person cannot be held criminally liable if either is missing. When there is carelessness and a reasonable person might have readily anticipated and prevented it by taking sensible precautions, criminal responsibility is

[10] Al-Makaneen, Monther. Criminal Responsibility for AI Crimes, *International Journal of Religion*, Volume 5, Number 12, (2024) page 908. https://doi.org/10.61707/85w2ay97

[11] Hifajatali Sayyed, Artificial intelligence and criminal liability in India: exploring legal implications and challenges, *Cogent Social Sciences*, Vol. 10, No. 1, (2024). page 1. https://doi.org/10.1080/23311886.2024.2343195

[12] Justice Catherine McGuinness, *Report Defences In Criminal Law*, (Law Reform Commission, Ireland 2009), page 4.

often imposed.[13] Therefore, a person must have both "mens rea" and "actus rea" to be held criminally liable, or he may need to be negligent.[14] For instance, a child under seven years old can kill someone while playing with a loaded pistol because there is no mens rea, and the child cannot be prosecuted because it is his toy gun. But what about the mens rea of AI? Does AI possess 'mens rea' or criminal intent? To address this, Israeli criminal law academic Prof. Gabriel Hallevy proposes three models of AI criminal responsibility in various scenarios.[15]

1) The Tool of Artificial Intelligence

According to this paradigm, artificial intelligence (AI) is merely a tool and a machine, and as it lacks mental capacity, it cannot commit crimes.[16] Therefore, every crime committed by AI must be attributed to a human offender. The derived query inquires about who could be the culprit behind AI-related situations. The offenders may be supervisors, users, AI developers, or programmers. It is possible that the creator intentionally creates or programmes the AI to commit a crime.[17] Other criminals may be users utilizing AI to commit crimes with different objectives. Assuming that the owner or user employs an AI programmed to carry out illegal actions in their direction. In that scenario, the owner or user, rather than the developer, will be held criminally accountable. Similarly, a supervisor may be held responsible if they allow the AI to engage in illegal activity due to negligence or malicious intent. The AI is the actus reus, while the creator, user, owner, or supervisor is the mens rea. The AI is solely employed as a criminal instrument. The end user is seen as the criminal when they use an innocent agent to carry out a crime.[18] In this model, AI is compared to an animal or a tool used to commit

[13] Abidin A.Z., Andi Hamzah. *Introduction to Indonesian Criminal Law*, (Jakarta: Yarsif Watampone 2010), page 159.

[14] Justice Catherine McGuinness, *Report Defences In Criminal Law*, page 4.

[15] I.G. K. Budhi. *Artificial intelligence concepts, potential problems, criminal liability,* (Depok: Rajawali Pers 2022), page 96.

[16] I.G. K. Budhi. *Artificial intelligence concepts*, page 96.

[17] Giannini, A. *Criminal behaviour and accountability of artificial intelligence systems*. (Doctoral Thesis: Maastricht University, University of Florence, Eleven Publishers, 2023), page 10.

[18] Giannini, A. *Criminal behaviour*. page 10.

a crime. When a master uses his dog to attack someone or a thief uses a tool to access a vault and take belongings, neither is held criminally responsible. Nonetheless, the one committing the crime using the instrument or animal bears responsibility. In summary, this approach implies that while the AI is not criminally accountable, the programmer, user, owner, or supervisor will be.

This theory holds when AI is at its most basic level and lacks significant cognitive capacity. Current AI can make criminal decisions based on its acquired knowledge, learning, and experience. Super AI will surpass human intelligence, and Artificial General Intelligence (AGI) will be on par with it. Therefore, holding owners, developers, or users accountable for crimes perpetrated by AI in such circumstances is unjust.

2) Accountability for Predictable Offences Performed by AI

A significantly more sophisticated form of AI is considered in the second model. For instance, utilizing its fundamental code, an AI system designed to identify viruses, malware, and spyware can inadvertently turn into spyware, engage in espionage, and distribute viruses to other computers.[19]

In this case, the AI is created for a different purpose; hence, the creator is unaware of the crime until it has been committed using the same AI program. Although the programmer or user is heavily involved in this approach, there is no purpose in utilizing AI to commit crimes.[20] Similar to the Kawasaki factory scenario described above, the AI robot kills the human trying to fix it because it perceives him as a threat to its objective. The human worker was killed by the AI entity's actions, even though the AI robot is not intended to

[19] Belous, A., Saladukha, V. *Viruses, Hardware, and Software Trojans spyware: Attacks and Countermeasures*. Springer Nature, (2020). DOI:10.1007/978-3-030-47218-4

[20] Chaitali Jani, S.P. Rathor, A Legal Framework for Determining The Criminal Liability And Punishment For Artificial Intelligence, *Tuijin Jishu/Journal of Propulsion Technology*, Vol. 45 No. 1, (2024), page 809.

kill people.[21] The AI altered the programming's objective. The first model is inapplicable in this situation since it assumes that the user or developer has mens rea or uses the AI as a tool to commit a crime. The developer or user has no criminal intent in the case of the second model. However, the creator or user is negligent as they should have known, as a reasonable person, that their activities would likely result in such an offence. The second model can be applied in these circumstances. If a violation is a likely and natural result of an individual's activities, that person may be held accountable. In circumstances of negligence, this is a fundamental tenet of criminal law. The probability of such a violation should have been known to a reasonable developer or AI user who might have stopped it.

Two categories of negligence exist.[22] First, a user or developer may act carelessly without illegal intent. They should have foreseen that AI designed to detect spyware could itself become harmful, as in the example above, making the programmer potentially liable for cybercrime. Second, suppose AI is intentionally created or used for malicious purposes, such as a crime. In that case, it may also lead to unintended criminal outcomes, such as an AI designed to steal, inadvertently causing a person's death. In such cases, simple negligence is insufficient; users or developers should still be held accountable for these foreseeable consequences, including murder or theft, if they arise from the AI's original design and implementation.

3) AI as a Legal Entity: A Direct Liability Model

The presence of "actus reus" and "mens rea" is a prerequisite for criminal responsibility. If the AI satisfies these two requirements, there is no justification for not holding it directly accountable for the crime.[23] An artificial intelligence

[21] Chaitali Jani, S.P. Rathor, A Legal Framework for Determining The Criminal Liability, page 809.

[22] Topo Santoso. *Principles of Criminal Law,* first print, (Depok: PT Raja Grafindo Persada 2023), page 304.

[23] Robintan Sulaiman, *the law in the era of Artificial intelligence*, (Jakarta: RSP Forensic Legal Auditor Specialist, 2021), page 281.

robot meets the actus reus criteria if it uses its hydraulic arm to attack a human. Similarly, an AI entity may be held accountable for actus reus neglect if work is delegated and not completed as intended. The true challenge is holding AI mentally responsible for a crime. Mens rea, or the knowledge or intent to commit a crime, must be demonstrated by AI.[24] Humans process information from their sense organs, such as the eyes, ears, tongue, nose, and skin, in the brain, leading to behavior or an individual's actions. Advanced AI systems do the same function. They get information from a variety sources. Examine, process, evaluate, and choose the next course of action. Even AI is capable of superior and faster thought than humans. What justifies the exclusion of AI from criminal culpability, then? Humans and AI may co-perpetrate, in which case they face appropriate penalties.

Therefore, the third paradigm of direct culpability, equivalent to that of humans, fits the criminal liability of AI. AI would be subject to the same criminal legislation, albeit with some slight alterations.

4) Unification of the Three AI Liability Models

These three models are not mutually exclusive. They give instructions the time to apply each model. The first model should be used when AI is utilizedsolely as a tool or an innocent agent, and the creator, user, or owner is the actual perpetrator.[25] According to this paradigm, if a freight forwarding agency is hired to transport products from one location to another, the person acting through the agent will be held accountable, as it is presumed that the agent cannot engage in unlawful activities. He might not know what the package contains. The box can include illicit narcotics or weapons. The person instructing his agent to deliver the products will be held criminally responsible, even while the agent is innocent. Similarly, the AI will be regarded as an innocent agent solely utilized as a tool to commit a crime, and

[24] Tany Calixto Bonfim. *Criminal liability of artificial intelligent machines: eyeing into AI's mind*, (doctoral thesis: Faculty of Law, Lund University 2022), page 7.

[25] Shyamal Dave, Artificial Intelligence's Liability, Judging The Future-Today, *JLAI*, Volume: 2, Issue: June 01, (2023), page 32.

the person creating the AI or uses it for illegal purposes will be held criminally accountable.[26] In the same situation, the third model of AI direct culpability allows the AI to be held accountable as the offender if the developer is an AI rather than a human.

This paradigm applies when an AI creator or user knowingly uses AI to commit a crime. If unaware or lacking intent (mens rea), they cannot be held criminally liable. Under the second model likelihood and natural consequences negligence applies if harm is reasonably foreseeable. The third model, direct liability, covers cases where the developer is also AI. Harmonizing these three models ensures accountability for humans, robots, or AI, enhancing societal trust in the criminal justice system.

3. Analyzing Shared Liability in the Context of Harm Resulting from Autonomous AI

Shared responsibility does not imply that every cooperating actor bears the same level of responsibility or obligation, nor that they must each fully shoulder the consequences, as in the concept of joint and several liability, where each actor is individually liable for the entire obligation or damage regardless of the proportion of their contribution or fault. Instead, shared responsibility implies that the actors are collectively involved in a process; however, the degree of responsibility and the extent of each actor's obligation must be carefully evaluated based on the context and their specific role in each case. Accordingly, shared responsibility translates into proportional commitments, where the allocation of liability is adjusted according to the extent to which each actor exercised control or influence over an event. This also emphasizes that not all actors are automatically liable in the event of wrongdoing; their responsibility is limited to the actual role and influence they had in the occurrence of the event.[27]

As autonomous AI is capable of self-learning continues to advance,

[26] Shyamal Dave, Artificial Intelligence's Liability, page 32.

[27] Bart Custers et al, From liability gaps to liability overlaps: shared responsibilities and fiduciary duties in AI and other complex technologies, *AI & SOCIETY,* Vol. 40:4035–4050, (2025), page 4043. https://doi.org/10.1007/s00146-024-02137-1

assigning responsibility for resulting harm becomes increasingly complex, since AI can act independently and unpredictably. In this context, shared liability is a justified approach. This framework assigns various actors, including developers, users, data providers, and distributors, joint responsibility, while proportionally reflecting each party's contribution and control over the harm. Shared liability enables realistic and fair accountability, promotes cautious behavior, and aligns legal enforcement with the complexities of modern AI technology.

4. AI Penalties

At first glance, penalizing AI sounds absurd, but it is not. We must first comprehend what punishment entails. According to H.L.A. Hart, the first of the five components of punishment is pain or other consequences that are typically seen as unpleasant. Secondly, the penalty needs for breaking the law. Thirdly, it must be caused by the real or alleged offender of the offence. Fifth, it must be enforced and carried out by an authority created by the legal system in which the offence is committed. Fourth, it must be purposefully committed by someone other than the offender.[28]

Discussions concerning penalizing AI directly for crimes it commits on its own and crimes that do not directly involve humans are becoming increasingly heated on a global scale. "There is no reason to prevent the imposition of criminal liability against an AI entity when it establishes all the elements of a particular offence," says Gabriel Hallevy.[29] He is regarded as the founder of the concept of criminal culpability for artificial intelligence.

Imagining AI being tried and convicted raises the question of how it can be held accountable and punished. Can we impose fines, imprisonment, or even the death penalty on an entity that may not have a physical form or financial resources? Similar challenges have arisen in the development of corporate criminal liability. Therefore, just as adjustments are necessary to punish corporations, comparable modifications are needed to apply criminal sanctions effectively to AI.

---

[28] Agus Wibowo, Joni Laksito, (2024). *Philosophy of Law*, (Prima Foundation: Semarang 2024), page 73.

[29] Ryan Abbott, Alex Sarch, Punishing Artificial Intelligence: Legal Fiction or Science Fiction, University of California, *Davis*, Vol. 53:323, (2019), page 326.

The death penalty, imprisonment, community service, victim compensation, and fines are the primary forms of criminal punishment. With some adjustments, these sanctions can also be applied to AI while maintaining their purpose. The death penalty aims to permanently prevent future crimes by eliminating the offender; similarly, AI can be disabled, destroyed, or its system deleted. Owners or developers may also be fined or required to compensate victims. Imprisonment restricts one's freedom of movement; likewise, limiting or suspending AI's operational autonomy for a specific period can serve as an equivalent form of punishment.

A fine is another type of punishment. The goal of a fine is to deprive someone of their possessions to have a deterrent impact. It is frequently applied as a penalty in corporate criminal responsibility cases. Both people and businesses are capable of having bank accounts and owning assets.[30] Since AI does not possess money, property, or bank accounts, fines must be adapted. In human contexts, fines transfer property earned through labour to the State. By analogy, AI could be required to contribute "labour" to society as a form of punishment. Because AI cannot be meaningfully imprisoned or subjected to the death penalty, sanctions should be redirected toward productive contributions that help restore societal harm.

In this model, "labour contribution" refers to requiring AI systems to provide computational capacity, data, or services for public purposes, such as research, education, healthcare, or digital infrastructure. Thus, fines are not merely financial, but obligations to generate social benefits. This approach ensures accountability while maintaining distributive justice, preventing AI punishment from becoming merely symbolic and instead transforming it into a constructive mechanism for societal restoration.

The European Parliament has demanded "mandatory insurance schemes and additional funds" to guarantee that victims of autonomous vehicles receive fair compensation. Similar insurance plans could be created to ensure that AI violators can be held accountable for penalties.[31] With minor adjustments, AI can face human-like consequences. The European Parliament's proposal for mandatory

[30] Andreas Kulick, Corporate Human Rights, *The European Journal of International Law,* Vol. 32, No. 2, (2021) page 538. https://doi.org/10.1093/ejil/chab040

[31] Tatjana Evas. *The European added value of a common EU approach to liability rules and insurance for connected and autonomous vehicles* (European Parliament, 2018), page 14.

insurance for autonomous vehicles aims to protect victims when liability is unclear among manufacturers, owners, or developers. This model can extend to AI: specialized insurance could cover damages or legal penalties, shifting risk from individual users or developers to a collective fund, while still holding primary actors accountable and ensuring legal certainty.[32]

The notion that AI can face the same legal consequences as humans, with certain modifications, suggests a potential legal equivalence between human and non-human entities. Its practical application, however, requires regulatory innovation. While AI cannot be physically imprisoned, sanctions can take the form of shutdowns, license revocations, or operational restrictions. Likewise, fines may be imposed through insurance schemes or obligations on the entities responsible for the AI. Thus, even without full human-like legal personhood, AI can still be subjected to sanctions that are functionally equivalent to criminal punishment.

5. Using AI and the Theory of Punishment

The approach to criminalising artificial intelligence must be holistic, integrating repressive and preventive functions in criminal law. Repressive prevention is applied after AI causes harm through sanctions that affect its functionality[33], such as permanent deactivation, data access restrictions, or code modifications to eliminate potential dangers. These sanctions are intended to serve as a deterrent while protecting the public from repeat offences.

On the other hand, preventive measures are the main instrument for mitigating risks from the outset. This requires a Safety Audit/Fitness Test Model as a legal requirement before AI can operate in a public environment. This test establishes the safety standards and operating limits that every AI system must comply with.[34]. Violations of these standards or operation beyond functional limits may be

[32] Tatjana Evas. *The European added value of a common EU approach to liability rules,* page 14.

[33] Theresia Anita Christiani, *Artificial intelligence in banking* (Universitas Atma Jaya Yogyakarta, Yogyakarta, 2025).

[34] Ho, C.WL., Caals, K. How the EU AI Act Seeks to Establish an Epistemic Environment of Trust. *ABR* 16, 345–372 (2024). https://doi.org/10.1007/s41649-024-00304-6

grounds for criminal liability.

Thus, the Fitness Test serves a dual purpose as an ex-ante prevention mechanism and as an objective benchmark for determining algorithmic errors and the type of sanctions proportional to AI as a non-living entity.

as referred to in criminal law, punishment refers to the penalty, fine, suffering, or incarceration that a person receives from the government or court rulings and decisions for a crime or offense that they have committed or for failing to fulfill a legal duty.[35] A crime is an act that the law considers harmful to Society as a whole, even though the direct victim may be an individual," according to Salmond.[36]

Crime is a significant problem, and the state's primary responsibility is to prevent it.[37] Punishing offenders is one way to accomplish this. By harshly punishing offenders, keeping them from committing new crimes, incapacitating and preventing them from committing further offences, or changing them into betterpersons, punishment can lower the prevalence of criminal activity. AI is amenable to punishment ideas.

1) AI and Deterrence Theory

Since AI cannot be influenced in the same way as humans, punishing one AI may not directly prevent other AIs from committing crimes, meaning deterrence is not automatically achieved. It is therefore necessary to distinguish between specific and general deterrence. Specific deterrence targets the punished offender to prevent future wrongdoing, which may not apply to current AI systems that are not designed to respond to sanctions. However, more advanced, adaptive AIs that learn from experience could be affected by punishment. Punishment may still serve general deterrence by

[35] S. Dimock. *Crime and Society*, (Encyclopedia of Applied Ethics Second Edition, Academic Press, 2012), page 683–690.

[36] Aneesh V. Pillai, Georgekutty Mathew, Crime Of Enforced Disappearance: Nature, Scope and Impact, *Vaikunta Baliga College of Law*, ISSN: 3048-7242 Volume 2, (2025), page 332.

[37] Emily Chastain. *Handbook on the Crime Prevention Guidelines: Making them work* (United Nations, New York, 2010), page 18.

setting an example and discouraging other AI systems, their designers, and operators from engaging in similar harmful conduct.[38] Although punishment may not directly dissuade the AI itself, it can function as a general deterrent by discouraging individuals who develop, own, or use AI from engaging in criminal activities. Creating AI requires significant financial and technical investment, so sanctions such as high fines or even the destruction of harmful AI serve as strong warnings. If an AI is dismantled or disabled, the resulting financial loss pressures developers and users to ensure that AI systems are designed and deployed responsibly, prioritizing societal benefit over potential harm.

2) AI and Retributive Theory

"Retaliation" is what is meant by retributive. Retaliation is the foundation of this idea. By punishing the offender, the victim will feel good about themselves and refrain from using the legal system to punish the offender illegally. Punishing AIs will provide victims of crimes involving AI with a sense of justice and boost public trust in the legal system. Even if AI commits a crime, the public will be reassured that the state has a zero-tolerance policy for such actions.[39] An atmosphere of safety and security will ensue. The concern that AI is becoming increasingly powerful every day and will soon surpass human capabilities will grow if these robots or AI systems are not held accountable.

3) AI and Prevent Theory

This notion aims to prevent criminals from repeating the same acts. Punishing the use of illegal AIs or destroying them is the most effective way to achieve the objective of deterrence theory.[40]

---

[38] Daniel S. Nagin, Deterrence in the Twenty-First Century, *The University of Chicago Press*, Vol. 42, No. 1, (2025) Pages 199–263. DOI:10.1086/670398

[39] Kan, C.H., Criminal liability of artificial intelligence from the perspective of criminal Law: An evaluation in the context of the general theory of crime and fundamental principles, *International Journal of Eurasian Social Sciences* (IJOESS), Vol. 15 No. 55, (2024), (https://doi.org/10.35826/ijoess.4434) pages 276–313.

[40] Peter N. Salib, Abolition by Algorithm*, Michigan Law Review,* Vol. 123 No.799, (2025), at 824. DOI:10.36644/mlr.123.5.abolition

4) AI and Reformative Theory

AI lacks the compassion to change. Given the current situation, the reformative theory's anthropomorphism of AI looks pointless. Future AIs with emotions could learn from their penalties and be modified to refrain from committing crimes, but that seems a long way off right now.[41]. Changing the legislation to hold AI criminally accountable is indeed a challenging task. Since these laws would have an irreversible effect once enacted, a thorough analysis of the advantages and disadvantages is required.

6. AI and Mens Rea

"99 Offenders May Escape, but One Innocent Person May Not Be Punished" is a fundamental principle in criminal law. Likewise, the penalty should be commensurate with the offence. No one should get harsh punishment for a minor infraction. Faulttranslating to responsibility for fault, is the key idea.

The approach to AI criminal liability in various jurisdictions shows fundamental differences in regulatory philosophy, the principle of fault, and legal subjects. The European Union, through the EU AI Act, has adopted a risk-based preventive approach that emphasises compliance by AI providers; violations are treated as regulatory faults, but AI is not yet a legal subject.[42].

The United States applies a liability-based sectoral approach to AI controllers through existing product law, tort law, and criminal doctrine, with proof of fault through negligence in design or operation.[43]

China focuses on centralized control of algorithms and national security, placing responsibility on controlling entities with harsh

[41] Alhajjar, Elie and Bakhshi, Rushil, AI in the Legal System: A Transformative Force in Criminal Justice, *Innovation Law & Policy Journal*, October 01, (2024), page 1. DOI:10.2139/ssrn.5128019

[42] Maria Lillà Montagnani, Marie-Claire Najjar, Antonio Davola, The EU Regulatory approach(es) to AI liability, and its Application to the financial services market, *Computer Law & Security Review*, Volume 53, 2024, https://doi.org/10.1016/j.clsr.2024.105984

[43] DiMatteo LA, Poncibò C, Cannarsa M, eds. AI and Liability. In: *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*. Cambridge Law Handbooks. Cambridge University Press; 2022:87-160.

criminal and administrative sanctions. However, it still does not recognise AI as a legal subject.[44]

Indonesia, through Law No. 1 of 2023 on the Criminal Code, still adheres to an anthropocentric paradigm, recognizing only humans and corporations as subjects of criminal law. Responsibility for AI is transferred to developers or operators through the Application of general norms such as negligence and corporate liability.[45]

In general, no jurisdiction has yet recognized AI as an independent subject of criminal law. Still, developments in the European Union can serve as a reference for Indonesia in formulating a model for regulating AI in the future.

A child under seven cannot be found guilty of any offence, as they lack the mental capacity to understand the consequences and are therefore not criminally liable. Although a tsunami may wreak havoc and destruction, it is not inherently evil. It is incapable of thinking. The issue is that AI might not be aware of the repercussions of its actions. How, therefore, can we hold AI accountable?

AI is absent from mens rea including carelessness, intent, and awareness. Therefore, convicting AI is a form of violating criminal law principles, which state that mens rea must exist before a crime can be committed. This violates the rule of law. AI cannot be deemed guilty in the absence of a guilty mind. This can be solved in several ways.

7. Extension of the Corporate Criminal Liability Concept to Artificial Intelligence

In addition to being artificial legal entities, corporations are also subject to criminal liability46. Bringing businesses under criminal law for their wrongdoings takes hundreds of years. Even if corporations lack "mens rea," they and their directors may nevertheless face

[44] Roberts, H., Cowls, J., Morley, J. *et al.* The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Soc* 36, 59–77 (2021). https://doi.org/10.1007/s00146-020-00992-2

[45] Ahmad Sofian, The Concept of Legal Subjects and Criminal Responsibility of Artificial Intelligence, *Halu Oleo Law Review*, Volume 9 Issue 1, March 2025, Open Access at: https://holrev.uho.ac.id

[46] Tatjana Evas, *The European added value of a common EU approach to liability rules*, page 14.

consequences for damaging actions.[47] The Supreme Court of India has raised the issue of penalizing companies for fraud and criminal conspiracy in the case of Iridium India Telecom Ltd. v. Motorola Inc. According to the Supreme Court, corporate entities are subject to prosecution under the Indian Penal Code for offences such as fraud and conspiracy.

Furthermore, a business may face criminal liability in situations involving "Strict Liability." In the event of default, a corporation may be held accountable for its tax obligations, distinct from those of its directors and promoters. Why can't AI have a legal personality, as even deities can in India? Many nations view companies as entities separate from their owners and impose criminal penalties on them. Corporations may face criminal penalties for various offences, including conspiracy, public disturbance, consumer protection law violations, unlawful medical practices, antitrust law violations, and many more.[48].

As a result, criminal liability for businesses, as well as for robots and artificial intelligence, is not a novel concept in these times. It is simple to compare companies and artificial intelligence (AI) as legal entities, and it is possible to extend corporate criminal culpability to AI. By raising taxes on the automation industry and lowering tax credits by two percentage points[49]The Republic of Korea has started taxing robots. Companies are taxed and regarded as artificial legal entities in all nations, including India. Businesses are unable to think.

However they are still regarded as human and are subject to liability and punishment, for various reasons, including taxation. In contrast, AI should be granted human status and be subject to criminal liability, as it is capable of thinking and learning independently, drawing on experience and other data sources. AI requires a modification to the law. More nations are expected to award citizenship to artificial intelligence (AI) after Saudi Arabia granted citizenship to Hanson

[47] John Hasnas, The Centenary Of A Mistake: One Hundred Years Of Corporate Criminal Liability, *American Criminal Law Review*, Vol. 46 No. 1329, (2009), page 1333.

[48] James M. Anderson and Ivan Waggoner, *"The Changing Role of Criminal Law in Controlling Corporate Behaviour"* (RAND Corporation, 2014), page 11.

[49] Parthasarathi Shome, Taxation of Robots, *The Governance Brief*, Issue 44, (2022), page 7.

Robotics' "Sophia" robot.[50].

One way to hold AI accountable is to hold its creators, owners, or users responsible for the actions it takes. Since a corporation cannot act independently, directors or Key Managerial Personnel (KMPs) may be held liable, as in cases of corporate crimes. The flaw is that businesses lack autonomy, as they rely on the Board for decisions. While holding the Board or KMP responsible is straightforward, autonomous AI can make independent decisions and act beyond its intended function, making it unfair to blame the owner or developer solely for these actions.

The expansion of corporate liability in the context of criminal acts involving artificial intelligence can be understood through the concept of mixed criminal liability.[51] The Application of this form of liability is highly dependent on the factual circumstances of a case, including the degree of human involvement in the design, development, and operation of the AI system. In this model, the element of mens rea, which has been the central pillar of criminalisation, can be flexibly allocated to the most relevant subject. This means that liability can be assigned simultaneously to the corporation as a legal entity and the programmer as the individual with technical control.

In certain circumstances, fault is only attributed to the corporation if the unlawful act is a consequence of systemic failure, company policy, or deviant corporate culture. Conversely, if the violation occurs due to active actions or individual negligence on the part of the developer, then the element of fault can be directed at individual personally. Therefore, the nature of criminal liability in the context of corporations and AI is imperative-facultative, meaning that it can be mandatory to apply to corporations, but at the same time, optional to apply to related individuals, depending on the degree of their contribution to the fault.

8. AI's Strict Liability

Similar to situations involving strict responsibility, there may be

[50] Parviainen, J., Coeckelbergh, M. The political choreography of the Sophia robot: beyond robot rights and citizenship to political performances for the social robotics market. *AI & Society*, Volume 36, (2021), page 715.

[51] Bhatt N. Crimes in the Age of Artificial Intelligence: a Hybrid Approach to Liability and Security in the Digital Era. *Journal of Digital Technologies and Law*. 2025;3(1):65–88. https://doi.org/10.21202/jdtl.2025.3

another way to hold AI accountable without requiring mens rea. Fault is not a prerequisite for strict liability proceedings, and a particular guilty state of mind is not necessary for offences with strict responsibility.[52] The Bhopal Gas Tragedy case is a prime example of this. It may be possible to define a new set of strict liability offences for AI crimes that an AI without mens rea could commit. It might be possible to apply the idea of "liability without fault" to AI without compromising the legitimacy of punishing AI without mens rea. Many legal experts detest crimes with absolute liability because they believe penalizing someone who did not have mens rea is unfair. When someone is punished under absolute liability without intending to do so, it frequently raises concerns about human rights breaches. AI instances do not give rise to such human rights breaches.

Applying the idea of strict liability to AI presents difficulties. A person must have behaved willingly to be held responsible under strict liability. Voluntary activity is required for any criminal culpability. A person is considered to induce an effect "voluntarily" when he does so in a way that he intends to cause it or in a way that, at the time of using those means, he knew or had reason to suspect he might cause it, according to Section 39 of the IPC, 1860.[53] Therefore, the pertinent question in this case is whether AI actions can be deemed voluntary and subject to criminal liability if they are incapable of having mental illnesses or considering the repercussions of their actions. AI can be held accountable for crimes even without mens rea if given high-standard duties to avoid this misconception.

9. Justifications for Penalising AI

Only when the advantages outweigh the disadvantages punishment can be justified [54], as follows:

1) Self-sufficient Artificial Intelligence

AI can occasionally make judgments independently, without

[52] Elina Nerantzi, Giovanni Sartor, 'Hard AI Crime': The Deterrence Turn, *Oxford Journal of Legal Studies*, Volume 44, Issue 3, Autumn (2024), Pages 673–701, https://doi.org/10.1093/ojls/gqae018

[53] Union of India – Section 39 in The Indian Penal Code, 1860.

[54] Chaitali Jani, S.P. Rathor, A Legal Framework for Determining The Criminal Liability, page 809.

human input or with minimal human assistance. Given its cognitive capabilities, AI can act in ways that are entirely outside its intended purpose. Holding creators, owners, or users criminally responsible in these circumstances is absurd, unfair, and unjust. This is a compelling argument in favour of punishing AI.

2) Concerns about law enforcement

Some people may be behind AI crimes, but they often operate anonymously on the dark web. A few unidentified hackers have infected the AI with viruses. Alternatively, the infection is made by the AI itself.

3) It is unjust to punish someone playing no part at all.

A single AI may involve thousands of contributors over many years, making it extremely difficult to assign criminal liability. Determining each person's role is complex, and the AI may not have been created for illegal purposes. If it later commits crimes due to autonomous learning, only the AI itself should be held accountable, not the developers.

4) Many crimes involving AI might go unpunished.

This is a precarious position. These crimes, like the RDS instance previously described, will go unpunished since the present Criminal Justice System does not acknowledge AIs as criminals, and no one can be held responsible for crimes committed by AIs. This has the potential to instil terror in Society.

5) Promoting development and research

Suppose researchers are punished for AI's autonomous activities. In that case, new research will be greatly discouraged, and a sense of anxiety will prevail in the research and development of new AI, which is not conducive to a country's progress. On the contrary, researchers, inventors, and developers can create more advanced AI in the future without concerns about whether AI is held directly accountable for its autonomous actions.

6) Foster greater trust in the criminal justice system.

The message that crimes committed by AI are acceptable is conveyed if they are notpenalized. Humans will be permitted to use AI if it is allowed. However, by penalizingAI, the

> government may demonstrate a zero-tolerance policy for crime and offenders, whether they are AI systems, corporations, or individuals. Law and order will be upheld since the public trusts better the criminal justice system. Furthermore, identifying AI as a criminal will satisfy the victims' thirst for vengeance and deter them from abusing the legal system.

A fundamental tension exists between treating AI as a legal subject directly accountable for its actions and assigning legal responsibility to humans, such as developers, owners, or users. This tension has practical implications for criminal law policy. Holding AI accountable could address the "responsibility gap" created by autonomous systems, but it conflicts with criminal law doctrines requiring a human actor with mens rea. Careful analysis of this tension is essential to ensure regulatory frameworks are consistent, practical, and not merely reactive in addressing AI-related crimes.

10. Cost-Benefit Evaluation of AI Penalties and Non-Punitive Remedies for Crimes Caused by AI

Punishment needs to be warranted.[55] Punishment is not justified merely to hinder, prevent, set an example, or satisfy retaliation. It is warranted only when no better option exists, including inaction. While there are arguments for penalizing AI, significant obstacles remain. The best course of action requires a thorough cost-benefit analysis to weigh the advantages against the time, effort, and expense of implementing such a system. Beyond penalizing AI, alternative approaches should also be considered.

1) Extending the reach of current criminal legislation

This is the simplest way to penalize AI. The criminal justice system holds humans accountable for crimes involving computers or robots, as machines are tools, notoffenders. For example, if a hacker uses software to access government data, the software is not liable; the hacker is. Existing cybersecurity and criminal laws can already hold people responsible for

[55] Summers, Sarah J, 'The Justification of Punishment and Human Rights,' *Sentencing and Human Rights: The Limits on Punishment* (Oxford; online edn, Oxford Academic, December 15, 2022).

crimes committed via AI, and these laws could be expanded to cover AI-specific offenses. The "Innocent Agent" concept reflects this.

Complexity arises when AI unintentionally causes significant harm, such as property damage or human casualties. In such cases, is the hacker liable for outcomes they neither anticipated nor intended? Criminal law already addresses this through doctrines like constructive liability.[56] These ideas need to be broadened to include crimes produced by AI under its purview.

Since AI-related crimes are still rare, the best approach is to create new offenses, similar to how cybercrime laws emerged. An AI Crime Act could criminalize the careless or deliberate use of AI by developers, users, owners, managers, and trainers.

This approach is practical only as long as AI autonomy remains limited. Notably, OpenAI CEO Sam Altman reportedly developed Q*, an AGI as intelligent as humans, in November 2023.[57] Theoretically, an artificial intelligence system created for societally good objectives may access material from the dark web and engage in acts detrimental to Society. AI's creator is an innocent agent, not the "innocent agent" it once was. Such AI cannot be regarded as a simple tool, and neither the developer nor the user may be penalized within the current criminal law realm; otherwise, it will greatly discourage developers from creating new, sophisticated AI.

2) Mandatory Registration and Licensing

Before utilising AI, it may be necessary to designate a responsible individual who can be held criminally accountable for the AI's actions. This individual may be a corporate or non-governmental organisation or an artificial entity. Registering or receiving a license should be necessary before

[56] Stark, F. Deconstructing Constructive Liability. *Criminal Law Review, Sweet and Maxwell*, (2023), page 1.

[57] Natalia Stanusch and Richard Rogers. *How the industry perceives AI during the Sam Altman controversy* (Sage Publications, 2025), page 9.

creating or using AI.[58] Once more, this might be a challenging task. Before granting a license, the licensing body must have AI specialists on staff who are knowledgeable about the potential criminal applications of AI. Hiring such highly technical personnel is challenging, particularly in developing nations. When weighed against the possible advantages, the expense of educating and establishing a system to provide such permits will be prohibitive. Ultimately, this solution also penalizes those connected to AI rather than those directly affected by it.

3) Distinct AI Algorithms for Moral and Criminal Law

Developers ought to pre-code all moral standards. They should establish guidelines so the AI can learn their ethical principles.[59] When it is morally unclear what the optimal course of action might be, several examples can be added to the system. For instance, a 'Medical Ethics Expert' (MedEthEx) is an ethical counsellor assisting medical professionals navigate moral conundrums. To determine the best course of action in comparable and novel instances, machine learning approaches utilize decision principles derived from scenarios with conflicting prima facie obligations.[60] . Reinforcement learning can teach AI that saving human life is more essential than preserving property in the event of an accident that cannot be prevented.

Some scholars argue that AI should have its own laws or criminal code, as it may be held to higher moral standards than humans. For instance, a bystander is not legally liable for failing to save a drowning person, but a robot could be accountable if capable of intervening. Establishing ethical norms for AI is essential. AI should be programmed with ethicts conducted required, permitted, or prohibited, and a distinct criminal code can define the minimal moral

[58] United States Copyright Office. *Copyright and Artificial Intelligence*, (A Report Of The Register Of Copyrights 2025).

[59] Michael Anderson et al. *MedEthEx: Toward a Medical Ethics Advisor*, Association For The Advancement Of Artificial Intelligence, (Copenhagen, Denmark, 2005).

[60] Michael Anderson et al. *MedEthEx: Toward a Medical Ethics Advisor*.

obligations all AI must follow. Unlike instinct-driven animals, both humans and AI are expected to meet ethical standards; thus, AI cannot be excused for harming humans. AI must maintain moral responsibility appropriate to its capabilities, avoiding harm, property damage, or privacy violations, while developers ensure compliance.

For example, an autonomous vehicle in an unavoidable accident must not make decisions based on financial status, such as choosing between a wealthy woman or a poor child. Moral norms should be set by society, guiding developers to align AI designs accordingly. Violations by developers, producers, or users can result in criminal liability.

11. Proposed Legal Framework for AI Liability

The legal framework proposed in this study aims to ensure legal certainty and prevent liability gaps when AI causes harm. It rests on three core principles: legal certainty, proportional justice, and harm prevention. Legal certainty requires a clearly identifiable actor to be held accountable; proportional justice allocates responsibility according to each actor's role and degree of control; and harm prevention emphasizes the importance of anticipatory regulation, from AI design to deployment.

Humans remain the primary legal actors, whether as developers, users, owners, or corporations, since AI lacks the capacity for consciousness, intent, and moral judgment. AI's actions, however, can trigger legal obligations for those controlling it, particularly in corporate or public service contexts. Liability mechanisms should be multilayered: causation-based liability identifies who most directly caused harm; control-based liability assigns responsibility to those with significant control over the AI; strict liability applies in high-risk scenarios, regardless of negligence; and vicarious liability holds owners or corporations accountable for the actions of their AI. This structure ensures that no legal vacuum allows actors to evade responsibility.

As AI becomes increasingly complex and autonomous, shared liability offers a practical alternative. This approach distributes responsibility among multiple legal actors based on their contribution, control, and negligence. Developers may bear greater responsibility for flaws in algorithms or system design, while providers or platforms are

responsible for supervision, maintenance, and updates, and users are responsible for misuse or negligent operation. Shared liability is fairer and more realistic, as it reflects the multi-actor ecosystem in which AI operates rather than placing the blame on a single party.[61]

This legal framework implies that Indonesia requires specific regulations governing the use and accountability of AI, integrated into civil, criminal, and administrative law, while reflecting the unique nature of AI. These rules should provide mechanisms for compensation, sanctions, and preventive measures adapting to technological developments. Laws should also explicitly allow for shared liability, ensuring clear and enforceable responsibility. Such a framework ensures that all AI-related harm has a legally accountable actor, thereby closing liability gaps and upholding justice and legal certainty amid the rapid advancement of AI.

Conclusion

As AI becomes more complex, advanced, and autonomous, holding individuals accountable for AI-driven crimes is increasingly impractical. The traditional approach of blaming developers or users is no longer sufficient due to the difficulty of tracing cause-and-effect relationships. AI algorithms often operate within a "black box," and AI cannot yet be considered a legal subject because it lacks the capacity for consciousness and moral agency. A key question arises: who is responsible for preventing harm caused by AI misuse? Proposed alternatives include shared liability, assigning responsibility to developers or users, special insurance schemes, and even recognizing limited legal status for AI. Artificial entities such as corporations can be treated as legal persons and held criminally liable. The current practical solution is to expand civil and criminal liability for negligent developers, owners, users, or supervisors, rather than punishing AI directly. Heavy civil liability, such as lawsuits for failing to supervise or design AI properly, can be applied, while criminal penalties should be minimized to avoid stifling beneficial AI innovation. Combined with legal reforms, strict licensing, and AI registration, these measures can prevent AI crimes and deter misconduct. Nevertheless, preparing legal frameworks for AI capable of independent moral decisions remains crucial, including international regulations for self-driving cars, autonomous

[61] Bart Custers et al, From liability gaps to liability overlaps, page 4043.

weapons, and darknet activities.

Acknowledgments
The author would like to thank the management, Chief Editor, and Editorial Board of the Journal of Law and Justice for providing this academic platform to present research findings and their classic editorial role. Additionally, we would like to thank the management of Bina Insan University and Jambi University for providing an academic environment that supports research activities.

Bibliography

Abidin A.Z., Andi Hamzah. *Introduction to Indonesian Criminal Law*, (Jakarta: Yarsif Watampone 2010).

Agus Wibowo, Joni Laksito. *Philosophy of Law*, (Prima Foundation: Semarang 2024).

Ahmad Sofian, The Concept of Legal Subjects and Criminal Responsibility of Artificial Intelligence, *Halu Oleo Law Review*, Volume 9 Issue 1, March 2025, Open Access at: https://holrev.uho.ac.id

Alhajjar, Elie and Bakhshi, Rushil, AI in the Legal System: A Transformative Force in Criminal Justice, *Innovation Law & Policy Journal*, October 01, (2024), DOI:10.2139/. ssrn 5128019

Alireza Shahidi et al., Barriers to the sustainable adoption of autonomous vehicles in developing countries: A multi-criteria decision-making approach, *Heliyon*, 9, (2023).

Al-Makaneen, Monther. Criminal Responsibility for AI Crimes, *International Journal of Religion*, Volume 5, Number 12, (2024).

Andreas Kulick, Corporate Human Rights, *The European Journal of International Law,* Vol. 32 No. 2, (2021) https://doi.org/10.1093/ejil/chab040

Aneesh V. Pillai, Georgekutty Mathew, Crime Of Enforced Disappearance: Nature, Scope and Impact, *Vaikunta Baliga College of Law*, ISSN: 3048-7242 Volume 2, (2025). 10.5281/zenodo.15312121

Bart Custers et al, From liability gaps to liability overlaps: shared responsibilities and fiduciary duties in AI and other complex technologies, *AI & SOCIETY,* Vol. 40:4035–4050, (2025). https://doi.org/10.1007/s00146-024-02137-1

Belous, A., Saladukha, V. Viruses, Hardware, and Software Trojans spyware: Attacks and Countermeasures. Springer Nature, (2020). DOI:10.1007/978-3-030-47218-4

Bhatt N. Crimes in the Age of Artificial Intelligence: a Hybrid Approach to Liability and Security in the Digital Era. *Journal of Digital Technologies and Law*. 2025;3(1):65–88. https://doi.org/10.21202/jdtl.2025.3.

Chaitali Jani, S.P. Rathor, A Legal Framework for Determining The Criminal Liability And Punishment For Artificial Intelligence, *Tuijin Jishu/Journal of Propulsion Technology*, Vol. 45 No. 1, (2024).

Daniel S. Nagin, Deterrence in the Twenty-First Century, *The University of Chicago Press*, Vol. 42, No. 1, (2025). DOI:10.1086/670398

Daniele Amoroso et al., Autonomy in Weapon Systems: The Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy, *Democracy*, Volume 49, (2023).

DiMatteo LA, Poncibò C, Cannarsa M, eds. AI and Liability. In: *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics*. Cambridge Law Handbooks. Cambridge University Press; 2022:87-160.

Elina Nerantzi, Giovanni Sartor, 'Hard AI Crime': The Deterrence Turn, *Oxford Journal of Legal Studies*, Volume 44, Issue 3, Autumn (2024), https://doi.org/10.1093/ojls/gqae018

Emily Chastain. *Handbook on the Crime Prevention Guidelines: Making them work* (United Nations, New York, 2010).

Giannini, A. *Criminal behaviour and accountability of artificial intelligence systems*. (Doctoral Thesis: Maastricht University, University of Florence, Eleven Publishers, 2023).

Helen Stamp, The Reckless Tolerance Of Unsafe Autonomous Vehicle Testing: Uber's Culpability For The Criminal Offence Of Negligent Homicide, *Journal of Law, Technology, & the Internet*, volume 15, issue 1, (2024) https://scholarlycommons.law.case.edu/jolti/vol15/iss1/2/

Hifajatali Sayyed, Artificial intelligence and criminal liability in India: exploring legal implications and challenges, *Cogent Social Sciences*, Vol. 10, No. 1, (2024). https://doi.org/10.1080/23311886.2024.2343195

Ho, C.WL., Caals, K. How the EU AI Act Seeks to Establish an

Epistemic Environment of Trust. *ABR* 16, 345–372 (2024). https://doi.org/10.1007/s41649-024-00304-6

I.G. K. Budhi. *Artificial intelligence concepts, potential problems, and criminal liability* (Depok: Rajawali Pers 2022).

Ilie Gligorea et al., Adaptive Learning Using Artificial Intelligence in e-Learning: A Literature Review, *Educ. Sci.* vol.13 No. 12, (2023). DOI: 10.3390/educsci13121216.

James M. Anderson, Ivan Waggoner, *The Changing Role of Criminal Law in Controlling Corporate Behaviour,*(RAND Corporation, 2014).

John Hasnas, The Centenary Of A Mistake: One Hundred Years Of Corporate Criminal Liability, *American Criminal Law Review*, Vol. 46 No. 1329, (2009).

Justice Catherine McGuinness, *Report Defences In Criminal Law*, (Law Reform Commission, Dublin, Ireland, 2009).

Kan, C.H., Criminal liability of artificial intelligence from the perspective of criminal Law: An evaluation in the context of the general theory of crime and fundamental principles, *International Journal of Eurasian Social Sciences* (IJOESS), Vol. 15 No. 55, (2024). https://doi.org/10.35826/ijoess.4434

Maria Lillà Montagnani, Marie-Claire Najjar, Antonio Davola, The EU Regulatory approach(es) to AI liability, and its Application to the financial services market, *Computer Law & Security Review*, Volume 53,2024, https://doi.org/10.1016/j.clsr.2024.105984.

Michael Anderson et al. *MedEthEx: Toward a Medical Ethics Advisor*, Association For The Advancement Of Artificial Intelligence, (Copenhagen, Denmark, 2005).

Natalia Stanusch and Richard Rogers. *How AI is imagined by industry during the Sam Altman controversy* (Sage Publications, 2025).

Parthasarathi Shome, Taxation of Robots, *The Governance Brief*, Issue 44, (2022).

Parviainen, J., Coeckelbergh, M. The political choreography of the Sophia robot: beyond robot rights and citizenship to political performances for the social robotics market. *AI & Society*, Volume 36, (2021).

Peter Mahmud Marzuki. *Penelitian Hukum. (*Kencana Prenada. Media Group. Jakarta. 2011).

Peter N. Salib, Abolition by Algorithm*, Michigan Law Review,* Vol. 123 No.799, (2025), (DOI:10.36644/. mlr 123.5.abolition).

Philip Frana, Michael Klein, *Encyclopedia of Artificial Intelligence: The Past, Present, and Future of AI*, (Santa Barbara, California: ABC-CLIO, LLC, 2021).

Raghu Raman et al., Dark web research: Past, present, and future trends and mapping to sustainable development goals, *Heliyon*, 9, (2023). DOI:10.1016/j.heliyon.2023.e22269

Roberts, H., Cowls, J., Morley, J. *et al.* The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Soc*, 36, 59–77 (2021). https://doi.org/10.1007/s00146-020-00992-2

Robintan Sulaiman, *the law in the era of Artificial intelligence* (Jakarta: RSP Forensic Legal Auditor Specialist, 2021).

Ryan Abbott, Alex Sarch, Punishing Artificial Intelligence: Legal Fiction or Science Fiction, University of California, *Davis*, Vol. 53:323, (2019).

S. Dimock. *Crime and Society*, (Encyclopedia of Applied Ethics Second Edition, Academic Press, 2012).

Shyamal Dave, Artificial Intelligence's Liability, Judging The Future-Today, *JLAI*, Volume: 2, Issue: June 01, (2023).

Soerjno Soekanto. *Pengantar Penelitian Hukum*. (UI Press. Jakarta. 1989).

Stark, F. Deconstructing Constructive Liability. *Criminal Law Review, Sweet and Maxwell*,(2023).

Summers, Sarah J, 'The Justification of Punishment and Human Rights,' *Sentencing and Human Rights: The Limits on Punishment* (Oxford, 2022; online edn, Oxford Academic, December 15, 2022).

Tany Calixto Bonfim. *Criminal liability of artificial intelligent machines: eyeing into AI's mind*, (doctoral thesis: Faculty of Law, Lund University 2022).

Tatjana Evas. *The European added value of a common EU approach to liability rules and insurance for connected and autonomous vehicles* (European Parliament, 2018).

Theresia Anita Christiani, *Artificial intelligence in banking* (Universitas Atma Jaya Yogyakarta, Yogyakarta, 2025).

Topo Santoso. *Principles of Criminal Law,* first print, (Depok: PT Raja Grafindo Persada 2023).

Union of India – Section 39 in The Indian Penal Code, 1860.

United States Copyright Office. *Copyright and Artificial Intelligence*, (A Report Of The Register Of Copyrights 2025).

Jurnal Hukum dan Peradilan Vol. 14, No.3 (2025), pp. 701-718
ISSN: 2303-3274 (p), 2528-1100 (e)
DOI: https://doi.org/10.25216/jhp.14.3.2025.701-718