Society Synergy Conference (SSC)
Volume II; Number II; Year 2025; Pages 728-737
Website:https://sinergilp.com
E-ISSN: 3048-3530

The Concept of Criminal Liability in Fraud Crimes Involving the Use of Artificial Intelligence

Rudi Salam Tarigan,*1 Azhali Siregar, *2 Rahmayanti *3

Email :tariganrudi21@gmail.com,azhalisiregar@dosen.pancabudi.ac.id,Rahmayanti@dosen.pancabudi.ac.id

[123] Universitas Pembangunan Panca Budi

Abstract

Advances in information technology have significantly impacted the modus operandi of criminal acts, particularly digital-based fraud. The use of Artificial Intelligence (AI) in cybercrimes, including fraud, poses new challenges for the criminal law system. This article aims to analyze the concept of criminal liability for perpetrators who use AI as a tool to commit fraud. The method used is normative research with a legislative and conceptual approach. The development of artificial intelligence (AI) technology has presented new challenges in the world of criminal law, particularly related to fraud. AI, originally designed to assist human activities, can now be misused as a tool to carry out fraudulent acts in increasingly complex and difficult-to-detect ways. The use of AI in these crimes not only changes the nature of the crime itself but also raises problems in determining criminal liability.

This study aims to examine the concept of criminal liability in fraud crimes involving artificial intelligence, both when AI is used as a tool by a human perpetrator and when AI operates autonomously, obscuring the perpetrator's identity. The primary focus of this study is an analysis of how Indonesian criminal law accommodates these cases within the current criminal liability framework. The method used in this research is a normative juridical method, with legislative, conceptual, and comparative approaches. This research also examines several international case studies and analyzes relevant legal literature. This is done to find common ground between conventional criminal law principles and disruptive digital technology developments.

Keywords: Criminal liability, fraud, artificial intelligence, cybercrime, criminal law

INTRODUCTION

The development of digital technology has revolutionized various aspects of human life, including crime. Fraud, once carried out conventionally, has now evolved into more complex and difficult-to-detect forms through digital media and AI-based devices. This phenomenon poses new challenges in the criminal justice system, particularly regarding the accountability of perpetrators who use advanced technology to disguise their identities and malicious intent. Therefore, it is crucial to reexamine the concept of criminal liability in the context of crimes involving AI. The development of information and communication technology has had a significant impact on various aspects of life, including the world of criminal law. One rapidly developing technology is artificial intelligence (AI), which has been implemented in various sectors, including finance, e-commerce, and public services.

Artificial intelligence is designed to mimic human thinking and decision-making through complex algorithms that continuously learn from data. However, its ability to act autonomously also raises new legal challenges, particularly when AI is used to commit or assist crimes, such as online fraud. Fraud crimes involving AI are becoming increasingly complex because perpetrators can use intelligent software to deceive, such as deepfakes, voice cloning, fraudulent chatbots, or automated phishing. In such situations, there is a blurring of the role of the human perpetrator and the actions of

CC Attribution-ShareAlike 4.0 License.

the AI system itself. The concept of criminal liability in conventional criminal law requires two main elements: actus reus (criminal act) and mens rea (malicious intent). However, AI, as a non-human entity, lacks will or intent, creating a dilemma in the application of criminal law. In cases where AI is used as a tool to commit fraud, it is necessary to investigate who can be held accountable. Is it the developer, the owner, the user, or another party indirectly involved in the use of the technology? This is a crucial point in constructing fair and proportionate criminal liability.

Countries around the world are currently grappling with the appropriate legal concept for dealing with technology-based crimes. In Europe, for example, discourse on "electronic personhood" for AI has emerged as an attempt to provide a legal framework for autonomous entities.[1]However, this approach has not been universally accepted. In Indonesia, criminal law still adheres to the principle of strict legality. This means that there is no crime without prior, clear legal regulations (nullum crimen sine lege). Therefore, dealing with AI-based fraud cases presents a unique challenge because the legal framework does not yet explicitly regulate the role of AI in criminal acts. In practice, law enforcement officials in Indonesia still focus on human actors who control or utilize AI to commit crimes. However, there is no legal formulation that specifically regulates how criminal responsibility is imposed if AI acts beyond control or has developed autonomously.

This research is crucial for delving deeper into the concept of criminal liability relevant to the development of AI, particularly in the context of fraud. An interdisciplinary approach combining criminal law, information technology, and technology ethics is needed. Furthermore, the formulation of new theories or the adaptation of existing criminal law theories is crucial. For example, can strict liability theory be applied in certain cases involving AI? Or might a corporate criminal law approach be necessary in this context?

The complexity of technology is also changing the relationship between perpetrators and victims. AI-based fraud is often widespread and transnational, raising issues of jurisdiction and coordination between countries in law enforcement. Furthermore, this issue concerns not only substantive criminal law but also formal criminal law, such as the use of evidence and electronic evidence. The role of AI in generating, deleting, or manipulating evidence presents new challenges for investigators and prosecutors. In the context of human rights, there are concerns that if AI is not strictly regulated, it could violate privacy rights or be used as a tool of repression. Therefore, the formulation of criminal liability must also consider the principles of justice, proportionality, and non-discrimination.

This research is expected to contribute scientifically to the development of Indonesian criminal law that is adaptive to technological advancements, without losing its essence of protecting the public and ensuring legal justice. Therefore, an in-depth analysis of the concept of criminal liability in fraudulent acts involving AI is necessary. This research will evaluate existing legal regulations, examine relevant legal theories, and provide conceptual proposals for reforming national criminal law.

Based on the background above, the problem formulation is as follows:

1) What is the concept of criminal liability in fraud crimes involving the use of Artificial Intelligence?
2) What are the Challenges and Legal Implications of Fraud Crimes Involving AI?

METHOD

This research is a normative legal study that utilizes a statute approach, a conceptual approach, and a case approach. Data sources were obtained from a literature review consisting of legislation, legal literature, and relevant journals and articles. The collected data were analyzed qualitatively, emphasizing legal logic and normative argumentation.

CC Attribution-ShareAlike 4.0 License.

RESULTS AND DISCUSSION

Artificial Intelligence and Its Automation Capabilities

AI is a computer system capable of performing tasks that require human intelligence, such as decision-making, pattern recognition, and learning. In a criminal context, AI can be used to create deepfakes, voice cloning, automated phishing, and even digital data manipulation. However, AI lacks free will (mens rea) or legal consciousness, and therefore cannot be held directly criminally liable. Artificial Intelligence (AI) is a branch of computer science that aims to create systems or machines that can mimic human thought processes, such as learning, problem-solving, and decision-making. AI is designed to perform tasks previously only capable of human intelligence, including facial recognition, natural language processing, and recommendation systems.

Along with technological advancements, AI has experienced rapid development in terms of automating various repetitive and complex activities. This automation capability allows AI systems to perform tasks without direct human intervention, thereby increasing efficiency and productivity in various sectors. AI-based automation can be found in various forms, such as robotic process automation (RPA), chatbots, autonomous vehicles, and machine learning algorithms in decision-making systems. This has transformed the way industries work, particularly in manufacturing, logistics, and customer service.

In the manufacturing industry, AI automation has replaced many manual tasks. Industrial robots equipped with AI can perform production processes continuously, with high precision, and adapt to changing production conditions. This provides advantages in terms of time and cost efficiency. In the healthcare sector, AI automation capabilities have been applied in disease diagnosis, medical record data processing, and even epidemic prediction. For example, AI algorithms can analyze MRI images to detect brain tumors more quickly and accurately than experienced radiologists.

One concrete example of AI automation is the use of chatbots in customer service. Using natural language processing (NLP) technology, chatbots can understand user questions and provide relevant answers without human intervention. In finance, AI has been applied in automated trading systems, fraud detection, and credit risk analysis. These systems can analyze millions of transactions in real time and automatically recognize suspicious patterns.

While AI automation brings many benefits, it also poses challenges, particularly in terms of replacing human labor. Many routine and predictive jobs are becoming irrelevant due to the replacement of intelligent machines, raising concerns about technological unemployment. On the other hand, AI automation also opens up new, more complex and highly skilled job opportunities, such as data scientists, AI engineers, and cybersecurity analysts. Therefore, adapting to technological change is crucial to bridge the skills gap.

It's important to note that AI automation isn't a total replacement for humans, but rather a collaboration between humans and machines (human-machine collaboration). AI is designed to enhance human capabilities, not completely replace them. Automation that relies too heavily on AI also carries ethical risks, such as algorithmic bias, data privacy violations, and opaque automated decision-making. Therefore, AI development must be accompanied by strict ethical principles and regulations. The development of AI in automation has also sparked philosophical debates about the limits of artificial intelligence and the capacity for machine consciousness. Whether AI capable of autonomous learning and adaptation can be considered "intelligent" in the true sense remains a long-standing debate among scientists.

Governments and educational institutions have a crucial role to play in preparing society for the wave of AI automation. Through technology-based curricula and digital skills training, people can be empowered to adapt to an increasingly digitalized workplace. With its expanding automation capabilities, AI has the potential to revolutionize various aspects of human life. However, like any other technology, the application of AI must be carried out wisely and responsibly so that its benefits can be felt equally and fairly. In conclusion, artificial intelligence and its automation capabilities have

CC Attribution-ShareAlike 4.0 License.

become a key pillar of the 21st-century digital transformation. While promising efficiency and progress, AI also demands social, economic, and ethical preparedness in its implementation. The future of AI is not only about technological sophistication, but also about how humans manage it wisely.

The Concept of Criminal Liability in Criminal Law for Fraud Crimes Involving AI

The development of information and communication technology has created a new era in society's social and economic systems. One of the most revolutionary innovations is artificial intelligence (AI), which has now penetrated various sectors, including finance, e-commerce, and public services. However, along with its benefits, there is also the risk of misuse of AI for criminal acts, including fraud.

The development of AI poses serious challenges to the criminal justice system, particularly in determining who is responsible. In cases of fraud involving AI, the fundamental question is who should be held criminally liable: the creator, the user, or the AI system itself. This creates a legal vacuum that urgently requires a response. The use of artificial intelligence has transformed the way criminals commit fraud. Now, perpetrators no longer need to interact face-to-face, as AI such as chatbots, deepfakes, or voice cloning can be used to defraud victims convincingly, quickly, and on a large scale. For example, perpetrators can use deepfake videos to pretend their boss is requesting an urgent cash transfer.

Fraud, according to Article 378 of the Criminal Code, is an act intended to unlawfully benefit oneself or another person, using a false name, deception, or a series of lies to induce another person to hand over goods or create debts/cancel receivables. When this element is carried out by an AI system, new challenges arise in proving and determining the perpetrator. The elements of deception and the act of inducing someone to hand over goods are fulfilled. However, in AI practice, this offense becomes material because the element of "deception" is difficult to prove when carried out by an autonomous system.

AI is used in various digital fraud schemes, such as automated phishing, voice cloning, deepfakes, and even fraudulent chat bots. Cases like CEO fraud involving AI voice imitation demonstrate that AI is no longer merely a passive tool. Debate has arisen over whether AI can be considered merely a tool or a perpetrator. In classical Indonesian criminal law, only humans or corporations can be held accountable. AI, while capable of learning and acting independently, does not yet have the status of a legal subject.

In Indonesian legal practice, criminal liability remains directed at humans, namely the creator, user, or party who directly benefits. The principles of culpa in eligendo and culpa in vigilando are used to target perpetrators who incorrectly select or fail to supervise their AI. Criminal liability in the Indonesian criminal law system is imposed on perpetrators who fulfill the elements of an unlawful act (actus reus) and fault (mens rea). In the context of AI use, the perpetrator is the party who has control over the AI system or who programs the AI to perform certain acts. Thus, humans remain legally responsible for the use of AI as a tool for crime.

Fraud is a fraudulent act committed to gain unlawful gain. In practice, AI is used to impersonate, spread false information, or simulate communication to deceive victims. Although AI technically carries out these actions, legal responsibility remains with the individual or group that initiates or utilizes the AI system. AI is used in various digital fraud schemes, such as automated phishing, voice cloning, deepfakes, and even fraudulent chat bots. Cases such as CEO fraud involving AI voice imitation demonstrate that AI is no longer merely a passive tool.

In classical criminal law, only humans (natural persons) or legal entities can be perpetrators of crimes. AI does not fall into this category. However, the autonomous nature and complex decision-making capabilities of AI raise the dilemma of whether it remains merely a "tool" or deserves to be treated as a responsible entity. According to the principle of legality in criminal law, there is no criminal act without a law governing it (nullum crimen sine lege). Therefore, the use of AI in crimes requires interpretation and even legal reform to adapt to new realities. Criminal liability encompasses

CC Attribution-ShareAlike 4.0 License.

two elements: the existence of an unlawful act and the perpetrator's capacity to be responsible (criminal responsibility). In the context of AI, this element is difficult to apply because AI lacks consciousness or free will, even though it can make decisions independently.

The element of fault (schuld) in criminal law is dolus (intentional) or culpa (negligence). In AI-based fraud, dolus is difficult to prove if the perpetrator conceals their involvement. Meanwhile, if the AI acts independently based on an algorithm, determining "fault" becomes a complex legal issue. If AI is considered a tool, then responsibility shifts to the human behind it, namely the creator, programmer, or user. This principle aligns with the theories of vicarious liability and indirect liability. However, the challenge is determining the perpetrator's level of knowledge and intent regarding the AI's actions.

In criminal law, the element of mens rea (malicious intent) is crucial for proving a crime. In AI that learns and develops on its own (machine learning), the developer may not be aware of all the actions the AI takes. Therefore, attributing intent to the perpetrator becomes problematic. The element of mens rea in fraud requires malice. When a perpetrator creates an AI system that then deceives people, we need to prove whether the perpetrator actually embedded that intent in the algorithm's design. However, in AI that uses unsupervised learning, this intent is difficult to prove directly.

The Criminal Code (KUHP) does not specifically regulate the use of AI in criminal acts. Therefore, approaches based on legal analogy and systematic interpretation are temporary solutions. However, this approach has limitations in addressing the rapidly evolving technical aspects of AI. Some academics have proposed the concept of electronic personhood for AI, allowing accountability to be directly attributed to the system. The European Union considered this in 2017, but it was widely rejected due to its perceived ethical and legal risks.

The United States and European Union countries are currently developing AI regulations, such as the Artificial Intelligence Act. In some jurisdictions, AI users can be held liable if proven negligent in their oversight or control of their systems. If errors occur due to negligence in the AI's design, such as allowing it to access data and generate deceptive output, the perpetrator can be charged with culpa or negligence. For example, an e-commerce AI that automatically displays fake promotions due to poor algorithm settings. Proving AI fraud is highly complex, involving code analysis, system logs, and algorithm audits. This requires digital forensic expertise and collaboration between agencies, including investigators, IT experts, and prosecutors.

Indonesia needs to establish new criminal regulations or revise the Criminal Code to address crimes involving advanced technology, including AI. Without legal certainty, victims of AI fraud are likely to face a lack of justice. The use of AI in fraud demonstrates the need for adaptive criminal law to provide effective legal protection for the public, particularly consumers and digital transaction actors. Beyond the legal aspect, the use of AI in crime raises ethical issues. Is it fair to criminalize individuals for the actions of an autonomous system? This requires a multidisciplinary approach combining law, ethics, and technology. Strategies to combat AI crime must include digital literacy, monitoring AI use, and developing algorithmic audit systems. Strengthening cyber law and digital-based law enforcement is key. Collaboration between academics, policymakers, and law enforcement officials is crucial for formulating a concept of criminal liability that adapts to developments in AI. This also provides space for the development of contemporary criminal law theory. The concept of criminal liability in fraud involving AI still faces numerous normative and technical challenges. Legal reform and an interdisciplinary approach are needed so that the legal system can adapt to technological developments in a proportional and fair manner.

Challenges and Legal Implications of Fraud Crimes Involving AI

The development of artificial intelligence (AI) technology has had a significant impact on various aspects of life, including criminal law. On the one hand, AI offers efficiency and convenience in carrying out economic and social activities. However, on the other hand, AI also poses potential threats in the form of fraudulent acts that are more complex and difficult to detect than previous conventional methods. The main problem in this context is the difficulty in proving the guilt of

CC Attribution-ShareAlike 4.0 License.

perpetrators who use AI to disguise their digital footprints. Furthermore, the lack of specific regulations regarding the use of AI in criminal acts complicates the law enforcement process. The development of adaptive criminal law doctrines and updates to legislation governing the use of technology in criminal acts are needed.

Fraudulent acts involving AI are often committed through data manipulation schemes, digital identity forgery, deepfakes, fraudulent chatbots, and automated system programming to deceive users. These crimes often do not involve direct human actors, but are instead perpetrated by systems programmed for malicious purposes. One of the main challenges in addressing AI-based fraudulent acts is the difficulty in determining who is legally responsible. Is the AI creator, the AI user, or the AI itself responsible? In criminal law, the principle of criminal responsibility requires a subject with legal awareness and free will, which AI lacks.

Furthermore, AI is autonomous and can learn on its own through machine learning mechanisms, so in some cases, fraudulent actions carried out by AI may not be directly programmed by its creator. This raises the problem of attribution of fault, as it is difficult to prove who directly perpetrated or initiated the fraud. Deepfake technology, which is the result of AI engineering to create fake videos or audio that closely resemble the original, has been used in various fraud modes, from impersonating officials to solicit money transfers to video call-based fraud. Detecting and proving authenticity in such cases requires advanced digital forensic expertise.

Law enforcement also faces obstacles due to limited evidence and difficulties in digital tracking. AI can hide its digital footprints very effectively through encryption and the use of hidden networks (the dark web), making it difficult for law enforcement officials to identify the true perpetrators. In the Indonesian context, the Criminal Code and specific laws such as the Electronic Information and Transactions Law (UU ITE) do not explicitly regulate legal liability for crimes involving AI. This indicates a legal vacuum that needs to be immediately filled with regulations that adapt to technological developments.

AI fraud is also often transnational, given that information technology recognizes no jurisdictional boundaries. This creates challenges in international cooperation, extradition, and tracing criminal assets held abroad. Victim protection is also a major challenge. Many victims of AI fraud are lay people who lack adequate digital literacy, making them easily deceived by AI systems that pretend to act like real humans. This requires public education and strengthening the community's digital literacy. Another crucial aspect is oversight of AI technology developers and providers. Regulations are needed that require AI developers to apply principles of security, ethics, and transparency in the design and use of AI to prevent its misuse for criminal purposes.

The application of due diligence and compliance principles in companies using AI is also crucial. Many business entities use AI to automate services but fail to audit the potential misuse of their systems, thus opening up opportunities for fraud by third parties. Efforts to prevent AI-based fraud require collaboration between government agencies, the private sector, and the public. The government needs to provide regulations and digital security infrastructure, while the private sector is required to implement early detection systems for potential AI misuse. From an academic perspective, interdisciplinary research combining law, technology, and criminology is needed to comprehensively understand the characteristics of AI crimes and develop appropriate legal approaches to address them. It is also important to highlight that the use of AI by law enforcement agencies themselves must be developed as a countermeasure to AI fraud. Examples include the use of deepfake detection systems, AI forensic tools, and digital transaction tracking algorithms that can expedite the investigation process. Thus, the challenges in dealing with fraud involving AI are complex, both in terms of substantive law, evidence, law enforcement, and victim protection. Therefore, legal reforms, institutional capacity building, and technology-based mitigation strategies are needed to effectively address this threat.

Another legal implication concerns the evidentiary aspect. AI can be used to erase digital traces or manipulate electronic evidence. As a result, the evidentiary process in court becomes more difficult, requiring high-level digital forensic expertise and a legal system that adapts to technological

CC Attribution-ShareAlike 4.0 License.

developments. Furthermore, the advent of AI also raises the need for criminal law reform in the context of cybercrime. Regulations governing digital fraud must be adapted to the realities of AI use, including the possibility of AI acting as a tool or perpetrator in crimes. Several developed countries, such as the European Union, have begun drafting regulations, such as the AI Act, which aims to regulate legal liability in the use of AI. Meanwhile, in Indonesia, academic discourse on the need for legal reform to address the challenges of AI has begun to emerge, but has not yet been translated into concrete policies.

Legal implications also touch on the protection of personal data. Many cases of fraud involving AI utilize data obtained illegally through information system breaches. This violates individuals' privacy rights, making robust data protection regulations crucial. The implications of AI extend beyond criminal law to civil and administrative law, such as civil liability for losses caused by AI, as well as the need for ethical standards and technology certification to prevent misuse. However, criminal law remains the primary instrument for responding to fraudulent acts that cause significant harm to society.

It should also be noted that the presence of AI in fraud crimes can widen the justice gap. Perpetrators of crimes involving AI typically have access to advanced technological resources, while victims are often ordinary citizens who lack adequate digital protection or understanding. These legal implications require the creation of a regulatory framework that is not only responsive but also preventative. Lawmakers must consider the technological aspects of every criminal offense, including the type of AI used, the perpetrator's intent, and the resulting social impact. Law enforcement against AI-based crimes must also involve cooperation between countries, particularly in cross-border investigations. AI allows perpetrators to commit crimes from one country and have repercussions in another, making national jurisdictions often insufficient to address them effectively. Thus, the legal implications of fraud crimes involving AI are broad, encompassing substantive, procedural, institutional, and public policy aspects. Synergy between policymakers, law enforcement officials, academics, and the technology sector is needed to formulate effective legal strategies. Efforts to reform the law and strengthen the criminal justice system are imperative to address the challenges of the digital era. Clear regulations, strict oversight, and public digital literacy are key to minimizing the negative impact of AI use in fraudulent activities.

CONCLUSION

1. Conclusion

1) The development of artificial intelligence (AI) has had a significant impact on various aspects of life, including criminal methods such as fraud. AI is exploited by criminals to impersonate, manipulate information, and simulate communication automatically and convincingly, making it an effective and difficult-to-detect fraud tool. Although AI can act autonomously, the current Indonesian criminal law system does not yet recognize AI as a legal subject, so criminal liability remains with humans, such as creators, users, or parties who benefit from the use of AI. Regulatory reform is needed, either through revisions to the Criminal Code or specific regulations governing the use of AI technology in criminal acts. This legal reform must be accompanied by an interdisciplinary approach that combines legal, technological, and ethical aspects to create a fair and proportional criminal accountability system. Furthermore, increasing the capacity of law enforcement, cross-sectoral collaboration, and strengthening public digital literacy are crucial to effectively anticipate and address AI-based crimes. Without adaptive legal reform, the risk of a normative vacuum and legal uncertainty in handling AI fraud will continue to increase.
2) The development of artificial intelligence (AI) has created new challenges in combating fraud. AI not only expands the methods of crime by creating more sophisticated fraud schemes, such as data manipulation, deepfakes, and fraudulent chatbots, but also creates complexities in terms of proof, attribution of fault, and determining legal liability. The autonomous, adaptive nature of AI, which can conceal digital traces, demands a more

CC Attribution-ShareAlike 4.0 License.

responsive legal system and advanced forensic technology to effectively address it. Responses to this threat must be carried out through a multidisciplinary and collaborative approach. The state needs to immediately fill the legal gap through adaptive regulations, establish principles of legal accountability for the use of AI, and strengthen the capacity of law enforcement officials. Meanwhile, protecting victims and increasing the public's digital literacy are also crucial aspects of the strategy for combating AI-based crimes. Criminal law reform, increased international cooperation, and the application of ethical principles in technology development are key foundations for maintaining a balance between technological progress and legal protection in the digital era.

2. Suggestion

1) To address the legal challenges posed by the misuse of artificial intelligence (AI) in fraud, a comprehensive overhaul of criminal regulations is necessary. The government and lawmakers must immediately draft or revise existing laws and regulations, including the Criminal Code, to accommodate modern technology-based crimes. Furthermore, increasing the capacity of law enforcement officers in digital forensics, algorithm audits, and technological literacy is crucial for effective evidence-gathering and law enforcement. It is crucial to maintain human agency as the primary legal subject in criminal liability, given that AI lacks will and legal awareness. The use of the precautionary principle, strict oversight of AI development and implementation, and interdisciplinary collaboration between legal, technological, and ethical experts need to be strengthened. With these steps, the Indonesian criminal justice system can transform into one that is adaptive, preventative, and continues to uphold justice in the digital era.
2) Given the complexity of the problems posed by the use of artificial intelligence (AI) in fraud, it is recommended that the government immediately formulate regulations specifically governing criminal liability in the use of AI. These regulations should include the identification of legally accountable entities, the classification of AI-based criminal acts, and ethical boundaries in the development and use of such technology. Furthermore, updates to the Criminal Code (KUHP) and the ITE Law are needed to be more responsive to developments in digital technology, including provisions on digital evidence and electronic forensic standards. In addition to regulations, it is also recommended to strengthen human resource capacity in law enforcement through digital forensics training, mastery of AI detection technology, and the establishment of a special cybercrime unit based on advanced technology. Collaboration between countries must also be strengthened to address jurisdictional challenges in cross-border fraud using AI. From a societal perspective, strengthening digital literacy and public education on AI-based fraud methods is essential to raise awareness and vigilance. The private sector, particularly technology developers, should also be required to apply principles of security, transparency, and ethics in the design of AI systems to prevent misuse.

BIBLIOGRAPHY

Andi Hamzah, Principles of Criminal Law, Jakarta: Rineka Cipta, 2008

Andi Hamzah, Introduction to Indonesian Criminal Law, Jakarta: Ghalia Indonesia, 2008.

Barda Nawawi Arief, Anthology of Criminal Law Policy, Jakarta: Prenada Media, 2008

Barda Nawawi Arief, Problems of Law Enforcement and Criminal Law Policy, Jakarta: Kencana, 2010.

Barda Nawawi Arief, Problems of Law Enforcement and Criminal Law Policy (Jakarta: Kencana, 2010).

Brenner, S. W. (2010). Cybercrime and the Law. New York: Routledge

Brenner, S. W. (2010). Cybercrime: Criminal Threats from Cyberspace. Santa Barbara: Praeger

CC Attribution-ShareAlike 4.0 License.

Brenner, Susan. Cybercrime: Criminal Threats from Cyberspace. Greenwood Publishing Group, 2010.

Brent D. Mittelstadt et al., "The Ethics of Algorithms: Mapping the Debate," Big Data & Society, 2016

BSSN. (2022). National Cybersecurity Strategy 2022–2024. Jakarta: BSSN

Casey, Eoghan & Stellatos, Gerasimos, "The Impact of Artificial Intelligence on Digital Forensic Investigations," Forensic Science International, Vol. 289, 2018

Chesney, R., & Citron, D. (2019). "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review, 107(6).

Daniel Jurafsky & James H. Martin, Speech and Language Processing, 3rd ed. (Pearson, 2023).

Dwiyana, R. (2022). Cyber Crime and Technology Crime. Bandung: Refika Aditama

EOS Hiariej, Principles of Legality and Development of Criminal Law (Yogyakarta: Cahaya Atma Pustaka, 2009).

Eric Topol, Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again (Basic Books, 2019).

Erik Brynjolfsson & Andrew McAfee, The Second Machine Age (WW Norton & Company, 2014).

European Commission. (2021). Proposal for a Regulation Laying Down Harmonized Rules on Artificial Intelligence (AI Act)

European Parliament. "Civil Law Rules on Robotics." 2017/2103(INL).

Europol, "Malicious Uses and Abuses of Artificial Intelligence," 2023,

Floridi, L., & Cowls, J. (2019). "A Unified Framework of Five Principles for AI in Society", Harvard Data Science Review, 1(1)

Gless, S., Silverman, E. J., & Weigend, T. (2016). "If Robots Cause Harm, Who Is to Blame?", New Criminal Law Review, 19(3).

Hart, HLA Punishment and Responsibility. Oxford University Press, 1968.

Hiariej, EOS, Principles of Legality and Development of Criminal Law, Yogyakarta: Cahaya Atma Pustaka, 2009

Iskandar, F. "Legal Responsibility for the Use of AI Technology in Cybercrime." Journal of Digital Law Science, Vol. 2, No. 2, 2022.

Jerry Kaplan, Humans Need Not Apply (Yale University Press, 2015).

John Searle, "Minds, Brains, and Programs," Behavioral and Brain Sciences 3 (1980).

Klaus Schwab, The Fourth Industrial Revolution (World Economic Forum, 2016), p. 44–49

Ministry of Communication and Information Technology of the Republic of Indonesia. (2020). National Digital Literacy Guide. Jakarta: Ministry of Communication and Information Technology

Lilik Mulyadi, Criminal Law in Indonesia (Theory and Practice), Jakarta: Sinar Grafika, 2016

Luciano Floridi, The Ethics of Artificial Intelligence (Oxford University Press, 2022).

Martin Ford, Rise of the Robots: Technology and the Threat of a Jobless Future (Basic Books, 2015).

Max Tegmark, Life 3.0: Being Human in the Age of Artificial Intelligence (Knopf, 2017).

Melanie Arntz, Terry Gregory, & Ulrich Zierahn, "The Risk of Automation for Jobs in OECD Countries," OECD Social, Employment and Migration Working Papers, No. 189, 2016

Michael Kearns & Aaron Roth, The Ethical Algorithm, Oxford University Press, 2019

Moeljatno, Principles of Criminal Law, Jakarta: Bina Aksara, 1987

Muladi, Corporate Criminal Liability, Semarang: UNDIP Publishing Agency, 2005

Nick Bostrom, Superintelligence: Paths, Dangers, Strategies (Oxford University Press, 2014).

CC Attribution-ShareAlike 4.0 License.

OECD. (2021). Artificial Intelligence in Criminal Law. Paris: OECD Publishing
R. Soesilo, The Criminal Code (KUHP) and its Complete Commentaries Article by Article, Jakarta: Politeia, 1996
R. Wiyono, Cybercrime Law in Indonesia, Jakarta: Sinar Grafika, 2022
Rony, AF "Artificial Intelligence in the Perspective of Indonesian Criminal Law." IUS Law Journal, Vol. 9, No. 1, 2021.
Russell, Stuart & Peter Norvig. Artificial Intelligence: A Modern Approach. Pearson Education, 2020.
Sihombing, R. (2023). Law and Technology in the Digital Era. Yogyakarta: FH UGM Press
Simons, K. W. (2018). Rethinking Mental States, Criminal Law and Philosophy, 12(3).
Simons, Kenneth W. "The Concept of Strict Liability in Criminal Law." Boston University Law Review, 2006.
Solum, Lawrence B., "Legal Personhood for Artificial Intelligences," North Carolina Law Review, Vol. 70, 1992
Solum, Lawrence. "Artificial Intelligence and Legal Theory." Northwestern University Law Review, 2018.
Stuart J. Russell & Peter Norvig, Artificial Intelligence: A Modern Approach, 4th ed. (Pearson, 2021).
Susanti Adi Nugroho, "Artificial Intelligence and the Challenges of Legal Ethics," Journal of Technology Law, Vol. 5, No. 2, 2021.
Syahrul, M. "Challenges of Law Enforcement in the Digital Era." Journal of Law & Technology, Vol. 3, No. 1, 2021.
Teguh, M. (2023). Artificial Intelligence and Its Impact on Criminal Law. Jakarta: Genta Hukum
Thomas H. Davenport & Rajeev Ronanki, "Artificial Intelligence for the Real World," Harvard Business Review, Jan–Feb 2018.
Law Number 11 of 2008 concerning Electronic Information and Transactions in conjunction with Law Number 19 of 2016.
Law Number 27 of 2022 concerning Personal Data Protection
Law of the Republic of Indonesia Number 1 of 1946 concerning Criminal Law Regulations.
Law of the Republic of Indonesia Number 1 of 1946 concerning Criminal Law Regulations.
United Nations. Guiding Principles on Business and Human Rights, 2011
UNODC. (2021). Cybercrime and AI: Challenges and Legal Responses. Vienna: United Nations Office on Drugs and Crime
Wahyudi, D. (2021). Digital Forensics and Electronic Evidence. Surabaya: Airlangga Press
Wischmeyer, Thomas & Rademacher, Timo. "Regulating AI — A European Perspective," Common Market Law Review, Vol. 58, 2021
Yuval Noah Harari, Homo Deus: A Brief History of Tomorrow (Harper, 2017).

CC Attribution-ShareAlike 4.0 License.