

International Criminal Law Challenges Regarding The Misuse of Artificial Intelligence in Transnational Crime

Muhammad Kevin Loriz¹, Joko Setiyono²

^{1,2}Faculty of Law, Diponegoro University, Semarang, Indonesia

ABSTRACT: The development of Artificial Intelligence (AI) has brought significant benefits across various sectors; however, it has also created new risks in transnational crime. The misuse of AI can facilitate various cross-border criminal activities, including cyber fraud, data theft, the spread of disinformation, money laundering, and organized crime. This situation poses challenges to international criminal law due to difficulties in determining jurisdiction, criminal liability, and the harmonization of regulations among countries. This study aims to analyze the challenges faced by international criminal law in addressing the misuse of AI and to examine measures that can strengthen international cooperation in law enforcement. The findings indicate that the advancement of AI technology is progressing more rapidly than the development of legal regulations, thereby necessitating updates to international legal instruments, enhanced cooperation among states, and stronger oversight and accountability mechanisms for AI use. Therefore, international criminal law must adapt progressively to effectively anticipate and combat AI-based transnational crimes.

KEYWORDS: Artificial Intelligence, Internasional Criminal Law, Transnational Crime, Law Enforcement

I. INTRODUCTION

Advancements in information and communication technology have brought about significant changes in social, economic, political, and legal interaction patterns within global society. One of the most influential technological innovations of the 21st century is Artificial Intelligence (AI). AI is a technological system designed to emulate human intellectual capabilities such as learning (machine learning), problem-solving, pattern recognition, decision-making, and making predictions based on available data. The advent of AI has yielded substantial benefits across various sectors, including healthcare, education, transportation, industry, security, and government administration. AI's ability to process vast amounts of data rapidly and accurately makes it a crucial instrument in supporting digital transformation across many countries (Russell & Norvig, 2021).

In the context of globalization, AI has emerged as a key driver of increased efficiency and productivity across various sectors. International organizations, governments, and the private sector are racing to develop and implement AI technologies to enhance competitiveness and accelerate innovation. Indeed, AI is projected to be a primary engine of global economic growth in the coming decades. However, like other technological advancements, AI also entails negative consequences that cannot be overlooked. The increasingly sophisticated capabilities of AI create opportunities for individuals and groups to exploit the technology for activities that contravene international laws and norms (OECD, 2023).

The misuse of AI in various forms of crime has become an issue of increasing concern for the international community. AI technology, originally developed to enhance human well-being, can now be employed to commit criminal acts with a level of complexity far exceeding that of conventional methods. AI enables perpetrators to automate illegal activities, increase the precision of attacks, expand operational reach across borders, and conceal their identities from law enforcement agencies. This phenomenon demonstrates that the advancement of AI presents not only technological challenges but also legal issues requiring serious attention from nations worldwide (UNICRI, 2020).

One emerging threat resulting from the misuse of AI is the rise of transnational crime. Transnational crime refers to criminal offenses involving more than one country whether regarding the perpetrators, victims, locations of execution, or the resulting impact. A defining characteristic of transnational crime is its ability to cross national jurisdictional boundaries, thereby necessitating international cooperation for prevention and enforcement (United Nations, 2000). The evolution of digital technology has accelerated the transformation of various forms of transnational crime, including cybercrime, money laundering, human trafficking, narcotics trafficking, terrorist financing, electronic fraud, and other forms of economic crime.

In the digital era, AI has become a tool that enhances the effectiveness and efficiency of transnational criminal activities. Criminals leverage AI algorithms to automate data analysis, identify vulnerable targets, devise more effective psychological

International Criminal Law Challenges Regarding the Misuse of Artificial Intelligence in Transnational Crime

manipulation techniques, and execute cyberattacks that are difficult to detect. A prominent example is the use of deepfake technology an AI-driven tool capable of generating highly realistic fake images, videos, and audio. This technology can be exploited for financial fraud, defamation, political manipulation, extortion, and the global dissemination of disinformation (Chesney & Citron, 2019).

Beyond deepfakes, AI is also employed to develop intelligent malware capable of adapting to digital security systems. Unlike conventional malware, AI-driven malware can learn a target system's defense patterns and automatically adjust its attack strategy to evade detection. This capability makes cybercrime increasingly difficult for law enforcement agencies and cybersecurity institutions to combat. Furthermore, AI is used to manage botnet networks, execute more convincing phishing attacks, and create fabricated digital identities for use in various cross-border criminal activities (Europol, 2022).

These developments pose serious challenges for the international criminal justice system. Fundamentally, international criminal law is designed to regulate and address various forms of crime that possess a transnational dimension or threaten the interests of the international community. However, most current international criminal law instruments were drafted before AI technology reached its present level of sophistication. Consequently, a gap exists between technological advancements and the law's capacity to regulate and respond to the evolving forms of AI misuse (Cassese, 2013).

One of the primary challenges in international criminal law concerns the issue of criminal liability. In criminal law theory, criminal liability generally requires the presence of a criminal act (*actus reus*) and an element of culpability (*mens rea*). Yet, when a crime is committed involving an AI system possessing a certain degree of autonomy, the question arises as to who should be held accountable. Should liability rest with the AI system's developer, the technology user, the platform owner, or another party profiting from the AI's use? This complexity is further compounded when AI systems are capable of performing actions that cannot be fully predicted by humans (Pagallo, 2013).

Beyond the issue of criminal liability, the misuse of AI in transnational crime also raises jurisdictional challenges. Crimes involving AI often span multiple countries simultaneously. For instance, a perpetrator might develop AI software in one country, run it via servers located in another, and target victims scattered across the globe. This situation complicates the determination of which state has the authority to conduct investigations, prosecute, or enforce criminal judgments. Disparities in legal systems, evidentiary standards, and national policies regarding AI further complicate international law enforcement efforts (Council of Europe, 2001).

Another challenge concerns the evidentiary aspects of criminal proceedings. AI enables the creation of various forms of fabricated digital evidence that are difficult to distinguish from authentic material. Technologies such as deepfakes and synthetic media threaten the integrity of evidentiary systems, as they can be used to falsify video footage, audio recordings, and electronic documents. In the context of international criminal law, this can hinder the identification of perpetrators, obscure legal facts, and cast doubt on the validity of evidence presented in court (UNODC, 2021).

At the international level, various organizations have recognized the importance of establishing a regulatory framework capable of addressing the risks associated with AI misuse. Organizations such as the United Nations (UN), the Organisation for Economic Co-operation and Development (OECD), and the Council of Europe have developed principles and guidelines regarding responsible AI governance. However, to date, there is no international criminal law instrument that specifically and comprehensively regulates the use of AI in transnational crime. This regulatory void creates legal loopholes that perpetrators can exploit to evade legal accountability UNESCO, 2021).

Furthermore, the rapid pace of AI development often outstrips the ability of states to craft adaptive regulations. This phenomenon is known as "regulatory lag" a situation where the law trails behind technological advancements. In many instances, the legislative process is relatively time-consuming, whereas AI innovation proceeds exponentially. Consequently, many nations struggle to align their national legal frameworks with the challenges posed by AI technology. This misalignment ultimately undermines the effectiveness of international cooperation in combating AI-enabled transnational crime (Hildebrandt, 2020).

The urgency of addressing the challenges international criminal law faces regarding AI misuse has grown alongside the global community's increasing reliance on digital technology. Various international reports indicate that AI is being employed in increasingly sophisticated and organized criminal schemes. Transnational criminal organizations are leveraging AI to expand their operational networks, boost economic gains, and minimize the risk of detection by law enforcement agencies. Therefore, a legal approach is required that focuses not only on enforcement but also on prevention, oversight, and the strengthening of international cooperation (WEF, 2025).

Based on the foregoing, it is evident that the misuse of Artificial Intelligence in transnational crime constitutes a complex, multidimensional legal issue. AI has transformed the nature of modern crime by introducing new methods that are more effective, organized, and difficult to detect. Conversely, international criminal law continues to face limitations regarding the determination of criminal liability and jurisdiction, the assurance of effective evidentiary standards, and the establishment of adequate international cooperation mechanisms. Thus, examining the challenges international criminal law faces regarding AI misuse in transnational crime is crucial for identifying regulatory gaps, evaluating the effectiveness of existing international legal instruments, and formulating regulatory models that are more responsive to technological developments in the digital era.

II. RESEARCH METHOD

This study employs normative legal research, which examines legal norms, principles, doctrines, and regulations relevant to the legal issues under discussion (Marzuki, 2017). The research uses a statute approach by analyzing international legal instruments related to transnational crime, cybercrime, and artificial intelligence governance, including the United Nations Convention against Transnational Organized Crime (UNTOC), the Convention on Cybercrime (Budapest Convention), and various international soft-law instruments concerning artificial intelligence issued by the United Nations, UNESCO, OECD, and other international organizations.

In addition, a conceptual approach is applied to examine legal doctrines and scholarly perspectives concerning criminal liability, jurisdiction, accountability, and the regulation of artificial intelligence in international criminal law. The study also employs a comparative approach by reviewing the existing international legal framework and identifying regulatory gaps in addressing AI-enabled transnational crimes.

The legal materials used consist of primary legal materials, including international conventions, treaties, and international policy instruments related to artificial intelligence, cybercrime, and transnational crime. Secondary legal materials include books, scientific journals, research reports, policy papers, and other academic publications relevant to international criminal law and artificial intelligence governance. Data collection was conducted through library research, while the analysis was carried out qualitatively using descriptive-analytical methods to examine the adequacy of existing international legal frameworks in addressing the misuse of artificial intelligence in transnational crime.

III. RESULT AND DISCUSSION

A. Forms and Characteristics of Artificial Intelligence (AI) Misuse in Transnational Crime and Its Implications for the Evolution of Cross-Border Crime in the Digital Era

The development of Artificial Intelligence (AI) over the past few decades has brought about fundamental changes in various aspects of human life, including the fields of economics, education, healthcare, security, and communication. AI's ability to process vast amounts of data, recognize patterns, make predictions, and automatically generate content has created new opportunities to enhance efficiency and productivity across various sectors. However, alongside these benefits, the advancement of AI also presents significant risks, as the technology can be misused to commit various forms of crime, including transnational crimes that cross national jurisdictional boundaries. The misuse of AI in transnational crime refers to the use of artificial intelligence technology by individuals, organized criminal groups, or non-state actors to carry out unlawful acts that have cross-border impacts through the exploitation of digital technologies and global internet networks (UNODC, 2023).

One of the most prominent forms of AI misuse is its application in cybercrime, where perpetrators utilize AI algorithms to automate attacks on information systems, exploit security vulnerabilities, steal personal data, and develop malware capable of adapting to the digital defense mechanisms employed by targets (Europol, 2022).

Unlike conventional cybercrimes that require constant human intervention, the use of AI enables attacks to be carried out automatically, continuously, and on a much larger scale, thereby increasing effectiveness while lowering operational costs for perpetrators. Furthermore, the development of generative AI technology creates new opportunities for criminals to produce various forms of authentic-looking fake content such as documents, emails, voice recordings, images, and videos that are difficult to distinguish from the genuine articles (OECD, 2023). Deepfake technology, for instance, has become a widely discussed instrument in the context of transnational crime due to its ability to digitally manipulate a person's identity for purposes such as fraud, extortion, the dissemination of disinformation, or the manipulation of public opinion. Through this technology, perpetrators can create visual or audio recordings showing individuals doing or saying things that never actually occurred; these can then be used to damage reputations, influence political processes, or illicitly gain economic benefits (Europol, 2022).

The misuse of AI is also evident in increasingly sophisticated social engineering and phishing practices. With advanced data analysis capabilities, AI can gather and process information about potential victims from various digital sources including social media enabling the creation of highly personalized and convincing fraudulent messages. This has led to a significant increase in the success rate of phishing attacks, as victims are more likely to trust information that appears relevant to their identities and activities (Interpol, 2023). Additionally, AI is employed in cross-border money laundering activities through the analysis of financial transaction patterns, the use of synthetic identities, and the utilization of digital assets, all of which allow perpetrators to more effectively conceal the origins of illicit funds (FATF, 2021).

In the context of organized crime, AI can even be used to manage criminal networks operating across multiple countries by automating communication, risk analysis, and the coordination of illegal activities tasks that previously required significant human resources. This demonstrates that AI serves not merely as a tool for committing crimes but also as a force multiplier that enhances the capacity and effectiveness of transnational criminal organizations (UNODC, 2024). A key characteristic of AI misuse in transnational crime is its borderless nature. Unlike conventional crimes, which generally require the perpetrator's physical presence at a specific location, AI-based crimes can be committed from anywhere, provided there is internet access and adequate digital infrastructure (Council of Europe, 2023).

International Criminal Law Challenges Regarding the Misuse of Artificial Intelligence in Transnational Crime

A perpetrator can operate from one country, utilize servers located in another, and simultaneously target victims scattered across the globe. This characteristic poses a major challenge for law enforcement, as it involves multiple jurisdictions with differing legal systems, evidentiary standards, and cooperation mechanisms. Beyond its cross-border nature, AI-based crime is also characterized by a high degree of automation. AI's ability to perform tasks autonomously allows perpetrators to execute thousands or even millions of attack attempts in a very short time without requiring direct human intervention (WEF, 2024).

Another prominent characteristic is scalability the ability to expand the scope of criminal operations at relatively low additional cost. While perpetrators once had to recruit more members to expand criminal networks, AI now enables exponential increases in operational capacity through the use of software capable of continuous operation. Furthermore, AI possesses adaptive capabilities that make it harder for security systems to detect. Through machine learning techniques, AI systems can study the defensive patterns employed by targets and adjust attack methods to remain effective even after security systems have been updated.

These characteristics render AI-enabled crime more dynamic, flexible, and unpredictable than other forms of digital crime. The implications of AI misuse for the evolution of transnational crime in the digital era are vast and complex. First, AI contributes to the increasing complexity of transnational crime by enabling the integration of various criminal methods into a single, coordinated operation. For instance, a criminal network might employ AI to gather victim data, generate phishing messages, steal credentials, launder illicit proceeds via digital assets, and disseminate disinformation to hinder law enforcement investigations (Interpol, 2023).

Second, AI expands the scale and reach of crime, allowing its impact to be felt globally within a relatively short period. An attack on a nation's digital infrastructure, for instance, can disrupt public services, financial systems, and economic activities on a broad scale, potentially triggering a domino effect on other countries with economic and technological interdependencies. Third, the misuse of AI heightens risks to international cybersecurity, as the technology enables the creation of threats that surpass the defensive capabilities of many organizations and developing nations (ITU, 2024). Fourth, the rise of AI-enabled crime poses serious challenges to both national and international legal systems. Many existing regulations do not specifically address legal liability regarding the use of AI in criminal acts, particularly when the technology operates autonomously or involves multiple parties across various countries (UNESCO, 2021).

Ambiguities concerning jurisdiction, legal liability, and extradition mechanisms in AI-enabled crime cases can hinder law enforcement efforts and allow perpetrators to exploit regulatory loopholes. Fifth, the growing threat of transnational AI-enabled crime underscores the need for stronger international cooperation in cybersecurity, intelligence sharing, regulatory harmonization, and the capacity building of law enforcement agencies. International organizations and governments increasingly recognize that AI-enabled crime cannot be effectively addressed through a purely national approach; instead, it requires a collective response involving diverse stakeholders, including the private sector, academia, and civil society organizations G7 Hiroshima AI Process, 2023).

Thus, it is evident that the misuse of Artificial Intelligence in transnational crime not only reflects the transformation of criminal methods in the digital age but also signals the emergence of new challenges capable of fundamentally altering the global security landscape. AI's capacity to enhance the efficiency, speed, scale, and complexity of criminal activities makes it a primary driver in the evolution of cross-border crime in the 21st century; consequently, adaptive legal frameworks, policies, and international cooperation mechanisms are essential to anticipate and address the various risks it presents (UNODC, 2023).

B. Challenges for International Criminal Law in Regulating and Determining Criminal Liability for the Misuse of Artificial Intelligence (AI) in Transnational Crimes

The development of Artificial Intelligence (AI) as a key technology of the Industrial Revolution 4.0 era has brought numerous benefits to human life; however, it has simultaneously created new challenges for international criminal law systems, particularly regarding the regulation and determination of criminal liability for the misuse of such technology in transnational crimes. AI-enabled transnational crime is evolving alongside advancements in artificial intelligence capabilities such as data analysis, automated decision-making, machine learning, and the generation of digital content resembling human output. In this context, international criminal law faces a fundamental issue: most existing legal instruments were drafted before AI technology had significantly advanced, rendering them ill-equipped to address the characteristics of crimes involving autonomous systems and intelligent algorithms (UNODC, 2023). International instruments traditionally used to address cross-border crime such as the United Nations Convention against Transnational Organized Crime (UNTOC) and the Council of Europe Convention on Cybercrime (Budapest Convention) remain fundamentally focused on criminal acts committed by human perpetrators, rather than activities involving AI systems capable of independently performing specific functions (United Nations, 2000; Council of Europe, 2001).

Consequently, a normative gap has emerged between technological advancements and the capacity of international law to regulate the increasingly complex forms of AI misuse. A primary regulatory challenge is the absence of a uniform international legal definition of AI and the limits of its use in the context of criminal offenses. Each country adopts a different approach to defining, classifying, and regulating AI technology, resulting in regulatory fragmentation that could hinder cross-border law enforcement efforts (OECD, 2022). Another challenge concerns the concepts of criminal legal subjects and criminal liability within the international legal system. Traditionally, criminal law is predicated on the assumption that the perpetrator of a crime is a human being or a legal entity capable of possessing intent, consciousness, and the ability to comprehend the consequences of their actions.

International Criminal Law Challenges Regarding the Misuse of Artificial Intelligence in Transnational Crime

The elements of fault (*mens rea*) and the criminal act (*actus reus*) serve as the fundamental basis for establishing criminal liability. However, in the context of AI, issues arise when a system generates actions that neither developers nor users can fully predict, owing to the system's self-learning capabilities (Matthias, 2004).

This situation raises fundamental questions regarding who should be held accountable when AI is used to commit transnational crimes whether liability rests with the software developer, the AI system manufacturer, the technology owner, the operator, the end-user, or another party benefiting from the AI's use. This ambiguity demonstrates the limitations of conventional criminal liability concepts when applied to technologies possessing a degree of autonomy. Some legal experts argue that AI systems have created an "accountability gap"—a situation where harm or criminal consequences occur, yet it is difficult to identify a party that can be held legally accountable. The issue of the accountability gap is further complicated in the context of transnational crime, as the AI usage chain often involves multiple parties located in different countries. By way of illustration, an AI system might be developed by a company in one country, trained using data obtained from another, operated via servers located in a different jurisdiction, and utilized by perpetrators to simultaneously attack victims across multiple countries. In such a scenario, determining liability involves not only technical issues regarding causation but also questions of jurisdiction and conflicts of law between nations (Interpol, 2023).

Furthermore, the use of generative AI in creating deepfakes, executing automated phishing attacks, manipulating digital identities, and disseminating cross-border disinformation demonstrates that this technology can serve as an instrument for crime with far-reaching consequences, all without the perpetrator's direct involvement at every operational stage. This contrasts with the concept of the perpetrator in classical criminal law, which positions the human being as the primary actor who consciously commits a prohibited act. Consequently, various academics and international organizations have begun proposing the development of new criminal liability models capable of addressing parties who exercise control or oversight, or who make significant contributions to the use of AI in criminal activities (European Parliament, 2020).

Another challenge concerns proving the element of culpability in cases involving AI. In criminal law, culpability is a fundamental prerequisite for imposing criminal sanctions. However, when an action is carried out via an AI system capable of making decisions based on algorithms and learned data, it becomes difficult to establish the existence of intent, knowledge, or negligence on the part of specific actors. For instance, if an AI system employed in business operations generates an action that a third party subsequently exploits to commit a transnational crime, a rigorous analysis is required to determine whether the developer or user bears sufficient culpability to be held criminally liable (Hildebrandt, 2020).

This complexity is further compounded when AI employs deep learning models, resulting in decision-making processes that are difficult to explain transparently a phenomenon known as the "black box problem." Under such circumstances, law enforcement officials and judges may struggle to comprehend how an AI system reached a specific decision and to what extent that decision can be linked to the actions of a responsible human agent (Pasquale, 2015).

From the perspective of international criminal law, challenges regarding regulation and criminal liability are also influenced by the principle of state sovereignty and the diversity of national legal systems. Not all states possess the same level of readiness to regulate AI whether in terms of regulation, institutional frameworks, or technical capacity. Some nations have developed specific legal frameworks for AI, while others still rely on general regulations that do not specifically address the risks associated with the technology. These disparities make achieving international legal harmonization difficult, even though the nature of AI-driven transnational crime demands uniform legal standards for effective law enforcement (UNESCO, 2021).

In this context, various international organizations have advocated for the establishment of global principles regarding AI governance, covering aspects such as accountability, transparency, security, and the protection of human rights. However, most of these instruments remain "soft law" and lack the binding force characteristic of international treaties in the field of criminal law (UNESCO, 2021).

Consequently, the implementation of these principles relies heavily on the political will of individual states. Furthermore, the rapid evolution of AI technology often places international criminal law in a reactive rather than proactive position. Regulations are frequently enacted only after significant risks or harms have emerged, whereas technological innovation advances at a far greater pace. This situation presents an ongoing challenge for policymakers to formulate rules that are flexible enough to accommodate future technological developments without stifling innovations that benefit society (OECD, 2023).

Therefore, the challenge for international criminal law in regulating and establishing criminal liability for the misuse of AI in transnational crimes relates not only to the absence of adequate legal norms but also to conceptual issues concerning legal subjects, the element of culpability, causation, cross-border jurisdiction, and the harmonization of international regulations. Until comprehensive solutions are found for these issues, a gap will persist between the evolution of AI technology and the effectiveness of international criminal law in ensuring legal certainty, protecting victims, and establishing fair accountability for parties involved in the misuse of such technology (UNODC, 2023).

CONCLUSIONS

The misuse of Artificial Intelligence (AI) has transformed the characteristics and patterns of transnational crime in the digital era, rendering them more complex, organized, and difficult to detect. The utilization of AI in various forms of crime such as cyberattacks,

International Criminal Law Challenges Regarding the Misuse of Artificial Intelligence in Transnational Crime

deepfakes, phishing, data theft, money laundering, and the dissemination of disinformation demonstrates that this technology serves not merely as an aid but as a factor that enhances the effectiveness and scale of cross-border criminal activities. AI's inherent characteristics automation, adaptability, scalability, and a borderless nature enable perpetrators to conduct operations globally while facing relatively lower risks. This situation exacerbates threats to international cybersecurity and economic stability, while also challenging the effectiveness of national and international legal systems in addressing technology-driven transnational crime.

International criminal law continues to face fundamental challenges in regulating, establishing criminal liability for, and enforcing the law against the misuse of AI in transnational crimes. These challenges include the absence of an international legal instrument that specifically and comprehensively addresses AI misuse, regulatory disparities among nations, difficulties in identifying the party liable for criminal acts involving AI systems, and the complexities of establishing proof due to the autonomous and algorithm-based nature of AI. Furthermore, issues regarding cross-border jurisdiction, accountability gaps, and limited international legal harmonization further complicate law enforcement efforts. Consequently, there is a need for the updating and harmonization of international regulations, strengthened inter-state cooperation, capacity building for law enforcement officials, and the development of adaptive criminal liability models to ensure that international criminal law can provide legal certainty and effectively respond to the future evolution of AI-driven transnational crime.

ACKNOWLEDGMENT

The author would like to express gratitude to colleagues at the Faculty of Law, Diponegoro University, for being invaluable discussion partners in the preparation of this journal. The author would like to thank the reviewers and editors for their efforts in shaping this paper.

REFERENCES

- 1) Andreas Matthias. "The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata." *Ethics and Information Technology*, Vol. 6, No. 3, 2004.
- 2) Cassese, Antonio. *International Criminal Law*. 3rd ed. Oxford: Oxford University Press, 2013. Council of Europe. *Convention on Cybercrime (Budapest Convention)*. Budapest, 2001.
- 3) Council of Europe. *Cybercrime Convention Committee Reports*. Strasbourg: Council of Europe, 2023.
- 4) Council of Europe. *Explanatory Report to the Convention on Cybercrime*. Strasbourg: Council of Europe, 2001.
- 5) European Parliament. *Resolution on Civil Liability Regime for Artificial Intelligence*. Brussels: European Parliament, 2020.
- 6) Europol. *Facing Reality? Law Enforcement and the Challenge of Deepfakes*. The Hague: Europol, 2022.
- 7) Europol. *Tech Watch Flash: Deepfake Technology*. The Hague: Europol, 2022.
- 8) Europol Innovation Lab. *The Impact of Artificial Intelligence on Policing*. The Hague: Europol, 2022.
- 9) Financial Action Task Force (FATF). *Opportunities and Challenges of New Technologies for AML/CFT*. Paris: FATF, 2021.
- 10) Frank Pasquale. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press, 2015.
- 11) Group of Seven (G7). *Hiroshima AI Process Comprehensive Policy Framework*. Hiroshima: G7, 2023.
- 12) Hildebrandt, Mireille. *Law for Computer Scientists and Other Folk*. Oxford: Oxford University Press, 2020.
- 13) Interpol. *Global Crime Trend Report 2023*. Singapore: Interpol, 2023.
- 14) International Telecommunication Union (ITU). *Global Cybersecurity Outlook 2024*. Geneva: ITU, 2024.
- 15) Marzuki, M. *Penelitian hukum: Edisi revisi*. Jakarta: Prenada Media, 2017.
- 16) Organisation for Economic Co-operation and Development (OECD). *Artificial Intelligence, Digital Transformation and Society*. Paris: OECD Publishing, 2023.
- 17) Organisation for Economic Co-operation and Development (OECD). *OECD Artificial Intelligence Outlook 2023*. Paris: OECD Publishing, 2023.
- 18) Organisation for Economic Co-operation and Development (OECD). *OECD Framework for the Classification of AI Systems*. Paris: OECD Publishing, 2022.
- 19) Pagallo, Ugo. *The Laws of Robots: Crimes, Contracts, and Torts*. Dordrecht: Springer, 2013.
- 20) Russell, Stuart, dan Peter Norvig. *Artificial Intelligence: A Modern Approach*. 4th ed. Harlow: Pearson Education, 2021.
- 21) United Nations. *United Nations Convention against Transnational Organized Crime (UNTOC)*. New York: United Nations, 2000.
- 22) United Nations Educational, Scientific and Cultural Organization (UNESCO). *Recommendation on the Ethics of Artificial Intelligence*. Paris: UNESCO, 2021.
- 23) United Nations Interregional Crime and Justice Research Institute (UNICRI). *Artificial Intelligence and Robotics for Law Enforcement*. Turin: UNICRI, 2020.
- 24) United Nations Office on Drugs and Crime (UNODC). *Global Study on Cybercrime*. Vienna: UNODC, 2024.

International Criminal Law Challenges Regarding the Misuse of Artificial Intelligence in Transnational Crime

- 25) United Nations Office on Drugs and Crime (UNODC). The Use of Artificial Intelligence in Criminal Activities and by Law Enforcement. Vienna: UNODC, 2023.
- 26) United Nations Office on Drugs and Crime (UNODC). The Use of Artificial Intelligence in Criminal Justice Systems. Vienna: UNODC, 2021.
- 27) World Economic Forum (WEF). Global Risks Report 2024. Geneva: World Economic Forum, 2024.
- 28) World Economic Forum (WEF). Global Risks Report 2025. Geneva: World Economic Forum, 2025.



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